2012
November

AxTraxNG™

Access Control Management Software

Software Manual (Version 21.x)

ROSSLARE
SECURITY PRODUCTS

Copyright © 2012 by Rosslare. All rights reserved.

This manual and the information contained herein are proprietary to REL, RSP Inc. and/or their related companies and/or subsidiaries' (hereafter: "ROSSLARE"). Only ROSSLARE and its customers have the right to use the information.

No part of this manual may be re-produced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of ROSSLARE.

ROSSLARE owns patents and patent applications, trademarks, copyrights, or other intellectual property rights covering the subject matter in this manual.

TEXTS, IMAGES, AND ILLUSTRATIONS INCLUDING THEIR ARRANGEMENT IN THIS DOCUMENT ARE SUBJECT TO THE PROTECTION OF COPYRIGHT LAWS AND OTHER LEGAL RIGHTS WORLDWIDE. THEIR USE, REPRODUCTION, AND TRANSMITTAL TO THIRD PARTIES WITHOUT EXPRESS WRITTEN PERMISSION MAY RESULT IN LEGAL PROCEEDINGS.

The furnishing of this manual to any party does not give that party or any third party any license to these patents, trademarks, copyrights or other intellectual property rights, except as expressly provided in any written agreement of ROSSLARE.

ROSSLARE reserves the right to revise and change this document at any time, without being obliged to announce such revisions or changes beforehand or after the fact.

Table of Contents

1. Introduction 11
1.1 System Features 11
1.1.1 Access Control 11
1.1.2 Access Monitoring 12
1.1.3 Software Security 12
1.2 AxTraxNG™ Server and Client 12
1.3 Using this User Guide 13
2. Specifications and Requirements 14
2.1 System Capabilities 14
2.2 System Requirements 15
2.2.1 AxTraxNG™ Server and Client Requirements 15
2.2.2 SQL Express Server Requirements 15
3. Installation 16
3.1 Choosing an SQL Server 16
3.2 Preparing the AxTraxNG™ Installation 16
3.3 Installing AxTraxNG™ Client Software 18
3.4 Installing AxTraxNG™ Network Server Software 19
3.5 Installing AxTraxNG™ Watchdog 22
3.6 Video Enhancement for AC-525 Setup 23
3.7 Firewall Settings 24
3.8 SQL Server Settings 24
4. System Overview 25
4.1 Starting the Software 25
4.2 AxTraxNG™ Main Window 26
4.3 Menu Bar 27
4.3.1 File Menu 27
4.3.2 Tools Menu 27
4.3.3 View Menu 28

4.3.4 Help Menu 28
4.4 Toolbar 28
4.4.1 General Icons 28
4.4.2 General Network Icons 29
4.4.3 Network Icons 29
4.4.4 Panel Icons 29
4.4.5 Card\Users Icons 30
4.4.6 Reports Icons 30
4.4.7 Events Toolbar Icons 30
4.5 Tree View 32
4.5.1 AC Networks 32
4.5.2 Cameras 32
4.5.3 Timing 32
4.5.4 Groups 32
4.5.5 Global Antipassback 33
4.5.6 Users 33
4.5.7 Status Map 34
4.5.8 Reports 34
5. How to Set Up a Site 35
5.1 Adding Time Zones 35
5.2 Adding Holidays 36
5.3 Adding a Network 37
5.4 Adding Access Control Panels 41
5.4.1 General Panel Settings 42
5.4.2 Adding a Panel 42
5.4.3 Editing the Panel 45
5.5 Configuring the Doors 48
5.6 Configuring the Readers 50
5.6.1 General Tab 50
5.6.2 Options Tab 52
5.6.3 Access Event 53
5.7 Configuring the Inputs 54
5.8 Adding a Camera 55

5.9 Adding Panel Links 55
5.9.1 Creating a Fire Alarm Input 59
5.10 Creating Groups 60
5.10.1 Adding Access Groups 60
5.10.2 Adding Input Groups 61
5.10.3 Adding Output Groups 62
5.10.4 Defining Card + Card Groups 63
5.11 Adding Users and Cards 64
5.11.1 Setting Card Automation 66
5.12 Adding Departments, Users, and Visitors 67
5.12.1 Adding Departments 67
5.12.2 Adding Users 67
5.12.3 Adding Visitors 72
5.13 Adding Access Areas 73
5.14 Adding Global Antipassback Rules 74
5.15 Car Parking 75
5.15.1 Viewing and Editing Car Parking Counters 77
5.16 Adding Operators 78
5.17 Creating Elevator Control 79
5.18 Creating Status Maps 79
6. ViTrax™ Video Integration 82
6.1 Connecting to ViTrax™ Server 82
6.2 Adding a Camera to the AC-525 Panel 84
6.3 Linking a Camera to AxTrax 84
6.4 Conditioned Recording via Panel Links 87
6.5 Viewing Recorded Events 87
6.6 Automated ViTrax™ Camera Activation Options 90
6.6.1 Reader Access 90
6.6.2 Alarm Event 91
6.6.3 Camera Event 92
6.6.4 Door Warning Event 92
7. Manual Operation 94

7.1 Controlling the Door Manually 94
7.2 Changing the Reader Mode 95
7.3 Controlling Outputs Manually 96
7.4 Manually Disarming Inputs 97
7.5 Controlling Sirens Manually 98
7.6 Manually Update Firmware 98
8. AxTraxNG™ Reports 99
8.1 Immediate Reports 99
8.2 Archive Reports 100
8.2.1 Panels Events Reports 100
8.2.2 System AxTraxNG™ Events Report 100
8.2.3 Interactive Report 100
9. Administrator Operations 102
9.1 Setting the Time and Date 102
9.2 Downloading Failed Data 102
9.3 Testing User Counters 103
9.4 Maintaining the Database 103
9.5 AxTraxNG™ Options and Preferences 105
9.5.1 General Tab 105
9.5.2 User Custom Fields 106
9.6 Importing/Exporting User Data 107
9.7 AxTrax GUI View Options 108
A. Firewall Configuration 109
B. SQL Service Settings 113
C. Network Configuration 114
D. Restoring Factory Default Settings 119
E. Configuring User Counters 120
E.1 Resetting Counter on Panel Re-enable 120
F. Cross Platform Camera Setup 122
G. Enrolling Cards using MD-08 Desktop Reader 125

H. SQL Server Installation Troubleshoot 126

I. AxTrax.NET Watchdog 129

I.1 Common Info 130

I.2 Error Log Sending 130

I.3 DB Connection 132

I.4 Restart Server 133

J. Adding Custom Wiegand Formats 134

J.1 Representation 134

J.2 Facility Code 135

J.3 Authentication 135

J.4 Creating New Rules 135

List of Figures

Figure 1: AxTraxNG™ Packages Selection Screen 17
Figure 2: User Properties > General Tab 68

List of Tables

Table 1: AxTraxNG™ Client Main Window 26
Table 2: Add Network > Options Tab..... 38
Table 3: Add Network > Options Tab..... 41
Table 4: Door Controller>Panel Properties>General Tab..... 43
Table 5: Network > Panel Properties > Antipassback Tab 46
Table 6: Network > Panel Properties > Options Tab..... 46
Table 7: Network > Panel > Doors > Door Properties 48
Table 8: Network > Panel > Readers > Reader Properties > General Tab 51
Table 9: Network > Panel > Readers > Reader Properties > Options Tab 52
Table 10: Network > Panel > Readers > Reader Properties > Access Event Tab53
Table 11: Network > Panel > Inputs > Input Properties..... 54
Table 12: Network > Panel > Links > Add Link Window 55
Table 13: Cards > Add Users and Cards Window..... 64
Table 14: Departments/Users > Department > User Properties > General Tab 68
Table 15: Departments/Users > Department > User Properties > Codes Tab .. 70
Table 16: Departments/Users > Department > User Properties > Details Tab.. 71
Table 17: Departments/Users > Visitors > Add User > Visitor's Options Tab ... 72
Table 18: Network > Panel > Cameras > Camera Properties Window..... 87
Table 19: Events Toolbar > Cameras > Live Video Streaming Window..... 90
Table 20: Tools > Database > Available Databases 104
Table 21: Tools > Options > General Tab 105
Table 22: Tools > Options > User Custom Fields Tab 106
Table 23: Tools > Import/Export Data..... 107
Table 24: Watchdog > Error Log Sending Screen 130
Table 25: Watchdog > DB Connection Screen 132

Notice and Disclaimer

This manual's sole purpose is to assist installers and/or users in the safe and efficient installation and usage of the system and/or product, and/or software described herein.

BEFORE ATTEMPTING TO INSTALL AND/OR USE THE SYSTEM, THE INSTALLER AND THE USER MUST READ THIS MANUAL AND BECOME FAMILIAR WITH ALL SAFETY REQUIREMENTS AND OPERATING PROCEDURES.

- The system must not be used for purposes other than those for which it was designed.
- The use of the software associated with the system and/or product, if applicable, is subject to the terms of the license provided as part of the purchase documents.
- ROSSLARE ENTERPRISES LIMITED and/or its related companies and/or subsidiaries' (hereafter:"ROSSLARE") exclusive warranty and liability is limited to the warranty and liability statement provided in an appendix at the end of this document.
- This manual describes the maximum configuration of the system with the maximum number of functions, including future options. Therefore, not all functions described in this manual may be available in the specific system and/or product configuration you purchased.
- Incorrect operation or installation, or failure of the user to effectively maintain the system, relieves the manufacturer (and seller) from all or any responsibility for consequent noncompliance, damage, or injury.
- The text, images and graphics contained in the manual are for the purpose of illustration and reference only.
- In no event shall manufacturer be liable for any special, direct, indirect, incidental, consequential, exemplary or punitive damages (including, without limitation, any and all damages from business interruption, loss of profits or revenue, cost of capital or loss of use of any property or capital or injury).
- All graphics in this manual are for reference only, some deviation between the image(s) and the actual product may occur.
- All wiring diagrams are intended for reference only, the photograph or graphic of the PCB(s) are intended for clearer illustration and understanding of the product and may differ from the actual PCB(s).

1. Introduction

The AxTraxNG™ Access Control System is a complete Server-Client software management system for use with the AC-215, AC-225, AC-425, and AC-525 Access control panels.

The AxTraxNG™ Access Control System is user-friendly, intuitive, and rich in functionality. Using AxTraxNG™, you can configure door functionalities based on areas and time frame for different types of personnel and for varying alarm situations.

The AxTraxNG™ Access Control System can integrate with ViTrax, Video Surveillance software application. The main purpose of the integration is to enable video recording based on access control events and convenient playback.

This manual is compatible with AxTraxNG™ software Version 00.12.00 and above.

1.1 System Features

AxTraxNG™ makes it possible to control and monitor every aspect of access control on a site. The system includes a built-in software security system that controls access to the system database, and logs all performed operations. In addition, the system boasts the following Professional Grade features:

- User-friendly PC software with intuitive layout reduces the complexity of access control
- Manages user data, photo and information fields, access rights, alarms, strike time, and door mode, all from one central location
- Produces reports from acquired data, such as entry and exit times, as well as alarm types initiated by user, location, and time events
- Available in multiple languages and date formats
- Compatible with additional video management software modules from Rosslare – ViTrax
- Backward compatibility with VeriTrax AS-225 and AxTrax AS-525

1.1.1 Access Control

Access groups define access rights for every part of the site. Access rights are time dependent; for example, users in the "Mornings Only" access group can have access to certain areas of the site between 9 am and 12 pm only. Assign each individual user to an access group.

The system also stores an identification photograph and personal details for each user, as well as user specific access settings, such as antipassback immunity, requirements for an extended open door period, configurable special privileges, and triggered outputs.

1.1.2 Access Monitoring

The AxTraxNG™ software records every attempt to open a door within the site. Status maps show the state of every part of a facility, while an Events log records complete details of every time access is granted or denied for every door on a site, and records possible door tampering and forced entries.

AxTraxNG™ can also produce a variety of access reports, including usage reports, attendance records, and roll calls. Using the AxTraxNG™ Report Wizard, users can design their custom reports to meet their specific needs.

1.1.3 Software Security

Access to the AxTraxNG™ software is password controlled. It is possible to grant individually based restricted security rights for different operators, with access to only specified elements of the system or with read-only access.

1.2 AxTraxNG™ Server and Client

The AxTraxNG™ system includes both the AxTraxNG™ Server and the AxTraxNG™ Client software applications separately.

Install the AxTraxNG™ Server on the computer that controls the access control panels and manages the database.

Install the AxTraxNG™ client software on any PC from which you wish to access the system. One AxTraxNG™ server can serve an unlimited number of AxTraxNG™ clients.

AxTraxNG™ is based on a standard Client-Server architecture:

- Only the server connects to the database; the clients draw the information from the server
- Clients connect to the server using Serial communication (RS-485) or LAN remote communication technology
- The server runs as a Windows service by default
- The client software is based on dynamic docking technology

Important

It is highly recommended that you back up the system database to an external storage device once a week (see Section 9.4).

1.3 Using this User Guide

This user guide provides all the information required to start working with AxTraxNG™ software. Refer to the AC-215, AC-225, AC-425, or AC-525 hardware manuals for wiring and installation instructions.

The manual explains the following in detail:

- How to install the AxTraxNG™ server
- How to install the AxTraxNG™ client
- The basic functionality of AxTraxNG™
- How to set up a new site from the AxTraxNG™
- How to monitor and manage a site using the AxTraxNG™ client

2. Specifications and Requirements

2.1 System Capabilities

General	
Software Architecture	Client-Server
Database Type	SQL Server Express 2005, 2008
Max. Number of Users	• 30,000 per panel (AC225,AC425, AC525) • 5000 (AC215)
Max. Access Groups	Based on the maximum number of users, 30,000 x the number of panels
Max. Number of Time Zones	32
Max. Cards per User	15
Max. Number of Doors	8184
Max. Access Control Panels	1023
Antipassback	• Timed • Door • Global – across the entire facility
International Holiday Support	Up to 64 holidays

Networks	
Max. Number of Networks	Unlimited
Supported Access Control Panel Models	• AC-215 • AC-215 (SPV) • AC-215IP • AC-225 • AC-225 with MD-IO84 • AC-225 with MD-D02 • AC-425 • AC-425 with MD-IO84 • AC-425 with MD-D04 • AC-525 • AC-525 with MD-IO84 • AC-525 with MD-D02
Panel Networks Communication Interface	• Serial (RS-232/485) • TCP-IP • Modem

Networks	
Communication Speed	9600, 19200, 57600, and 115200 bps

2.2 System Requirements

2.2.1 AxTraxNG™ Server and Client Requirements

Operating System	Windows XP SP2, Windows Server 2003, Windows Server 2008 (32/64 bits), Windows Vista, or Windows 7 (32/64 bits)
Processor	Pentium 4 or better
Memory	4 GB
Network	LAN card required for TCP/IP networking
Hard Disk Space	4 GB minimum

2.2.2 SQL Express Server Requirements

SQL Server Express is not always required. See Section 3.1 for further information.

Processor	Pentium 4 or better
Memory	2 GB
Hard Disk Space	4 GB

3. Installation

The AxTraxNG™ installation CD-ROM includes all the setup files required to install the AxTraxNG™ Access Control software on the system's main computer. The software system consists of the following four main components:

- AxTraxNG™ Server – Manages the database linked to the access control panels
- AxTraxNG™ Client – Configures the system

  The AxTraxNG™ Client is only needed on the main computer; however, it can be installed on additional computers as needed to help monitor the system.
- ViTrax™ software – Enables video integration (if needed)
- AxTraxNG™ Watchdog

In addition, the setup installs the following two prerequisite applications:

- Crystal Reports Basic Runtime for Visual Studio 2008
- Microsoft® Visual C++ 2005 SP1

3.1 Choosing an SQL Server

The AxTraxNG™ Server operates using an SQL server 2005/2008 database. If there is already an SQL 2005/2008 server available on your computer network, use it to run the AxTraxNG™ database using your SQL login credentials.

Alternatively, install Microsoft SQL Server Express on the computer that uses the AxTraxNG™ server.

Do not install the SQL server when installing additional AxTraxNG™ clients, which connect to the AxTraxNG™ Server database.

3.2 Preparing the AxTraxNG™ Installation

Install the AxTraxNG™ Access Control software on the computer that connects to the access control panels and manages the database.

To begin installing the AxTraxNG™ software:

1. Insert the CD into your computer's CD drive.
2. Double-click the AxTraxNG™ setup file.

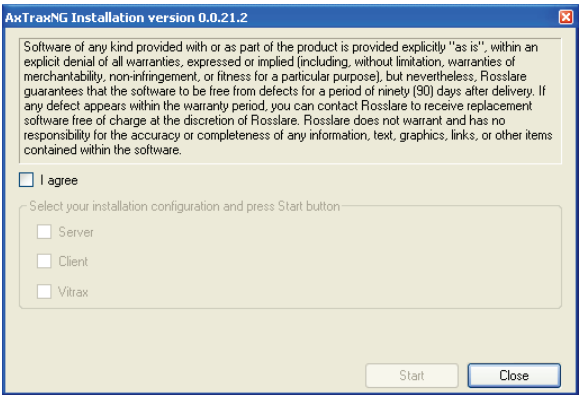
   The following verification screen opens:

Open File - Security Warning
The publisher could not be verified. Are you sure you want to run this software?
Name: AxTraxNGSetup_1_0.21.2_28_10_2012.exe
Publisher: Unknown Publisher
Type: Application
From: P:\Sam
Run
Cancel
Always ask before opening this file
This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?

3. Click **Run**.

   Once the various necessary files are extracted, the following screen opens:

Figure 1: AxTraxNG™ Packages Selection Screen


AxTraxNG Installation version 0.0.21.2
Software of any kind provided with or as part of the product is provided explicitly "as is", within an explicit denial of all warranties, expressed or implied (including, without limitation, warranties of merchantability, non-infringement, or fitness for a particular purpose), but nevertheless, Rosslare guarantees that the software to be free from defects for a period of ninety (90) days after delivery. If any defect appears within the warranty period, you can contact Rosslare to receive replacement software free of charge at the discretion of Rosslare. Rosslare does not warrant and has no responsibility for the accuracy or completeness of any information, text, graphics, links, or other items contained within the software.
I agree
Select your installation configuration and press Start button
Server
Client
Vitrax
Start
Close

Note

This screen remains opens in the background as various elements of the software are installed.

4. Accept the licensing agreement and choose which packages you wish to install.

Note

When installing the ViTrax™ software for video integration, make sure to install it on every client PC as well as on the server PC.

5. Click **Start**.

Note

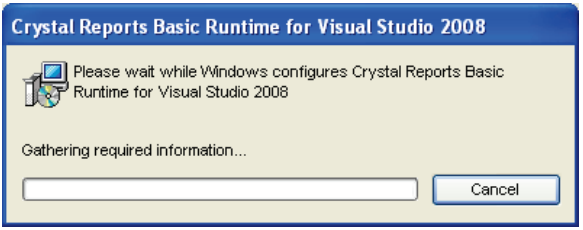
If the AxTraxNG™ Server or Client setup detects a previous version of AxTraxNG, a prompt appears asking if you want to upgrade AxTraxNG™ to the newer version.

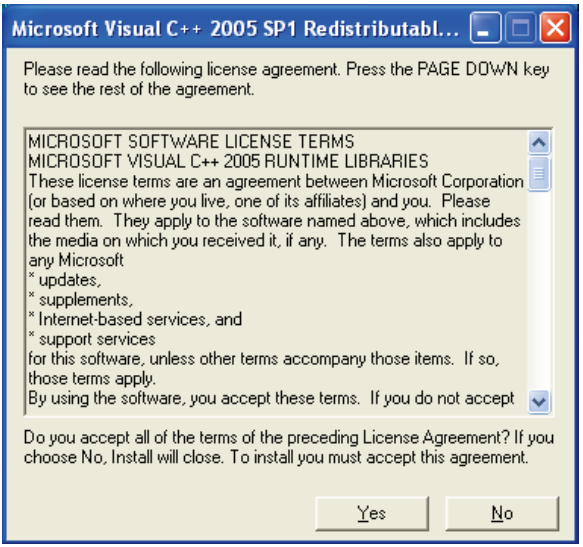
Upgrading to a newer version only uses current database information.

After upgrading the AxTraxNG™ version, check the panel's firmware version for both old and new installations and upgrade your firmware if required.

If there is no SQL server installed, the Installation Requirements screen opens.

The installation process of the two prerequisite applications begins.


Crystal Reports Basic Runtime for Visual Studio 2008
Please wait while Windows configures Crystal Reports Basic Runtime for Visual Studio 2008
Gathering required information...
Cancel

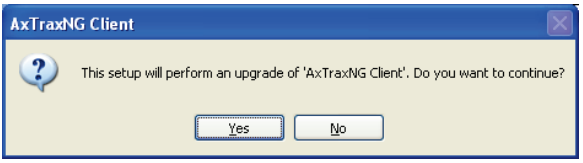

Microsoft Visual C++ 2005 SP1 Redistributabl...
Please read the following license agreement. Press the PAGE DOWN key to see the rest of the agreement.
MICROSOFT SOFTWARE LICENSE TERMS
MICROSOFT VISUAL C++ 2005 RUNTIME LIBRARIES
These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft
* updates,
* supplements,
* Internet-based services, and
* support services
for this software, unless other terms accompany those items. If so, those terms apply.
By using the software, you accept these terms. If you do not accept
Do you accept all of the terms of the preceding License Agreement? If you choose No, Install will close. To install you must accept this agreement.
Yes
No

Once these installations finish, the AxTraxNG™ Client installation begins.

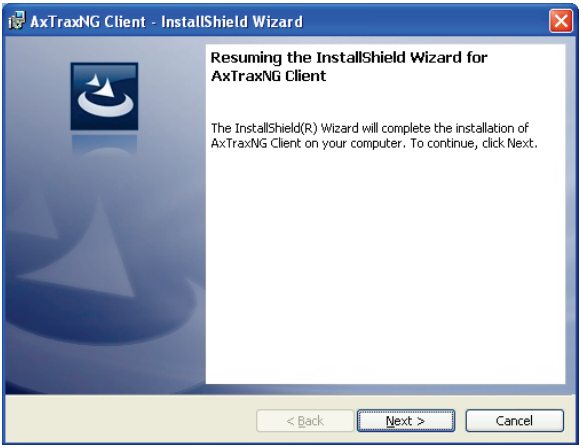
3.3 Installing AxTraxNG™ Client Software

The installation wizard opens automatically once the prerequisite software is installed.

If you are upgrading, the following screen opens:



If you are installing for the first time, the following screen opens:


AxTraxNG Client - InstallShield Wizard
Resuming the InstallShield Wizard for AxTraxNG Client
The InstallShield(R) Wizard will complete the installation of AxTraxNG Client on your computer. To continue, click Next.
< Back
Next >
Cancel

To install the AxTraxNG™ Client application:

1. Click **Yes** and/or **Next** to begin the AxTraxNG™ Client installation process.
2. If you are installing an upgrade, skip to Step 5.

   The *Destination Folder* screen opens.
3. Select the required installation location by clicking **Browse** or click **Next** to use the default destination

   The *Ready to Install the Program* screen opens.
4. Click **Install**.

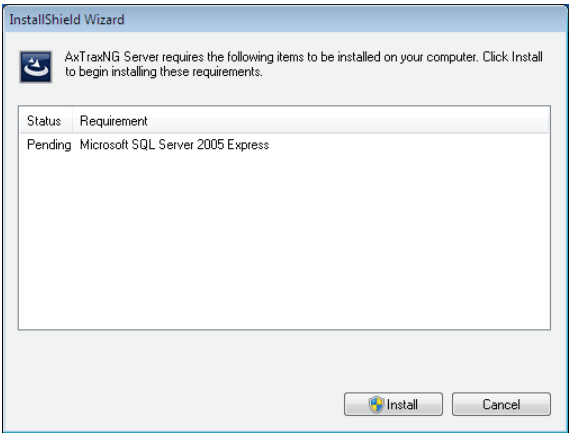
   The *Installing AxTraxNG™ Client* screen opens.

   When the installation is complete, the *InstallShield Wizard Completed* screen opens.
5. Click **Finish** to complete installing the AxTraxNG™ Client software.

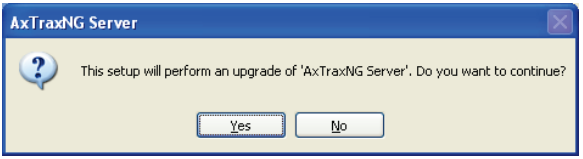
3.4 Installing AxTraxNG™ Network Server Software

Following the AxTraxNG™ Client software installations, the AxTraxNG™ Install Shield Wizard for the AxTraxNG™ Server software installation appears.

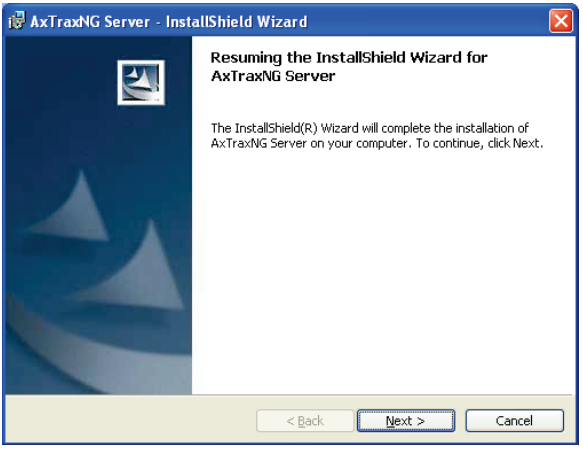
If there is no SQL server installed, the Installation Requirements screen opens. Click **Install** and follow the steps to install the SQL server.



If you are upgrading, the following screen opens:



If you are installing for the first time, the following screen opens:


AxTraxNG Server - InstallShield Wizard
Resuming the InstallShield Wizard for AxTraxNG Server
The InstallShield(R) Wizard will complete the installation of AxTraxNG Server on your computer. To continue, click Next.
< Back
Next >
Cancel

To install the AxTraxNG™ Server:

1. Click **Yes** and/or **Next** to begin the AxTraxNG™ Server installation process.
2. If you are installing an upgrade, skip to Step 10.
3. Click **Next**.

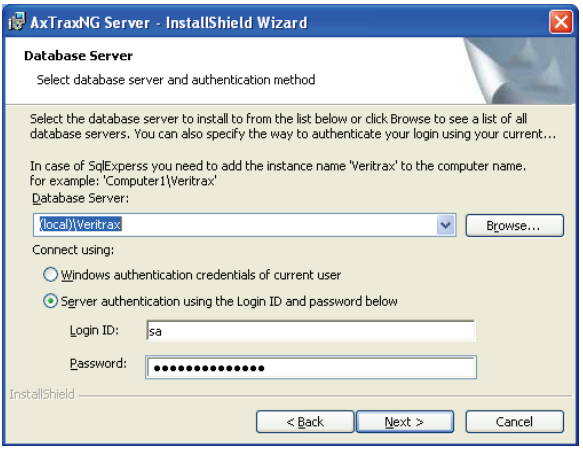
The *Setup Type* screen opens.

4. Select the **Server** option, and then click **Next**.

   The *Destination Folder* screen opens.

5. Select the required installation location by clicking **Browse** or click **Next** to use the default destination

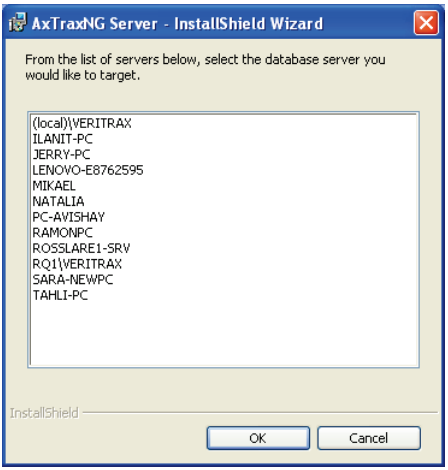
   The *Database Server* screen opens.


AxTraxNG Server - InstallShield Wizard
Database Server
Select database server and authentication method
Select the database server to install to from the list below or click Browse to see a list of all database servers. You can also specify the way to authenticate your login using your current...
In case of SqlExperss you need to add the instance name 'Veritrax' to the computer name. for example: 'Computer1\Veritrax'
Database Server:
(local)\Veritrax
Browse...
Connect using:
Windows authentication credentials of current user
Server authentication using the Login ID and password below
Login ID:
sa
Password:
InstallShield
< Back
Next >
Cancel

6. For the ***Database Server* field**, do one of the following**:**

   a. Select the database server name from the dropdown list or use the default location *(local)**Veritrax*.

   b. Click **Browse…** to choose the database server location.



The AxTraxNG™ Server and SQL Server databases must be installed on the same PC.

c. For database servers installed from the AxTraxNG™ Server setup program ("SQL Server express"), add the instance name "\VeriTrax" to the database computer name and click **OK**.

   You return to the previous window.

7. In **Connect using**, choose **Server authentication using the Login ID and password below**.

The only condition for choosing the **Windows authentication credentials of current user** option is that you are using an existing SQL database installed using Windows authentication only and not from the VeriTrax Setup.

8. Click **Next**.

   The Ready to Install the Program screen opens.

9. Click **Install**.

   The *Installing AxTraxNG™ Server* screen opens.

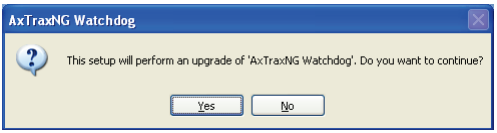
   When the installation is complete, the *Install Shield Wizard Completed* screen opens.

10. Click **Finish** to complete installing the AxTraxNG™ Server software.

3.5 Installing AxTraxNG™ Watchdog

Once the AxTraxNG™ server installation finishes, the AxTraxNG™ Watchdog installation opens automatically.

If you are upgrading, the following screen opens:



If you are installing for the first time, the following screen opens:

AxTraxNG Watchdog - InstallShield Wizard
Resuming the InstallShield Wizard for AxTraxNG Watchdog
The InstallShield(R) Wizard will complete the installation of AxTraxNG Watchdog on your computer. To continue, click Next.
< Back
Next >
Cancel

To install the AxTraxNG™ Watchdog:

1. Click **Yes** and/or **Next** to begin the AxTraxNG™ Watchdog installation process.
2. Click **Next** to initiate the AxTraxNG™ Watchdog installation process.

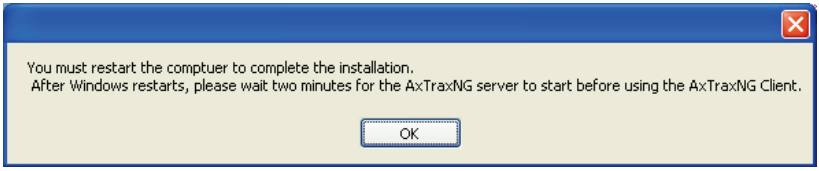
   The *Destination Folder* screen opens.
3. Select the required installation location by clicking **Browse** or click **Next** to use the default destination

   The *Ready to Install the Program* screen opens.
4. Click **Install**.

   The installation process begins.

   When the installation is complete, the *InstallShield Wizard Completed* screen opens.
5. Click **Finish** to complete the AxTraxNG™ Watchdog software installation.

   A window opens telling you to restart the computer.


You must restart the comptuer to complete the installation.
After Windows restarts, please wait two minutes for the AxTraxNG server to start before using the AxTraxNG Client.
OK

6. Click **OK**.
7. Return to the AxTraxNG™ Elements Selection Screen (Figure 1).
8. Click **Close** and then restart the computer.

The AxTraxNG™ server is now fully installed on your computer.

Once the computer restarts, you must wait until you see a message in the Windows system tray that the server is connected.

3.6 Video Enhancement for AC-525 Setup

AxTraxNG™ can connect with single or multiple ViTrax™ servers installed in a LAN or WAN configuration.

Note

Make sure to check AxTraxNG™ and ViTrax™ version compatibility.

To install ViTrax™ Server and Client applications, refer to the *ViTrax™ Software Installation Manual*.

When installing AxTraxNG™ on a different PC, make sure that the ViTrax™ Server has already been installed (no license is required for that ViTrax™ Server).

To add cameras for AC-525:

1. Activate the ViTrax™ Server and Client (see *ViTrax™ Software Installation Manual*).
2. Define ViTrax™ Servers (see Section 6.1).
3. Define communication of AC-525 cameras to the ViTrax™ Server (see Section 6.2).
4. Activate AxTraxNG™ and configure it (see Chapters 4 and 5).

3.7 Firewall Settings

Internal firewall settings may prevent the AxTraxNG™ Server from connecting to the SQL database or to panel control units using TCP/IP and remote Server-Client connection.

For more information on how to configure a firewall, see Appendix A. Contact your system administrator or Rosslare Technical Support for further guidance.

3.8 SQL Server Settings

After installing AxTraxNG™, verify that the SQL server service on the computer is running and set to the required installation.

For more information on SQL server settings, see Appendix B.

If SQL Express 2005 is being installed (part of the installation package), the installation must be on the same Windows user account that is being used for AxTraxNG™.

4. System Overview

AxTraxNG™ is controlled through a user-friendly interface, and comes with a Tree View list of all aspects of the site setup and a toolbar for standard operations.

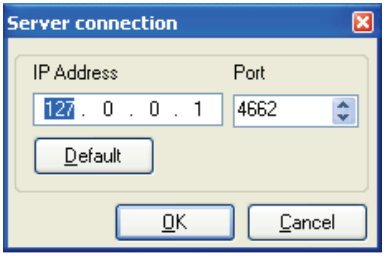
4.1 Starting the Software

This section explains how to start the software and log in to the main window.

To start AxTraxNG™:

1. Double-click the AxTraxNG™ Client icon ( ) on the desktop, or select the program from the Rosslare folder in the Start menu.

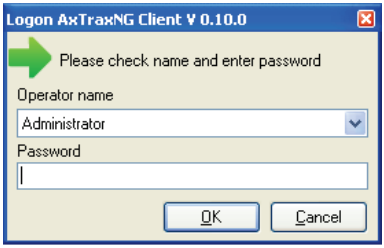
   If the AxTraxNG™ server is installed on a different PC, the Server connection dialog box appears.



   If the AxTraxNG™ server is installed on the same PC, skip to Step 5 (after the *Logon AxTraxNG™ Client* Dialog box appears).

2. Type the AxTraxNG™ server's PC IP address in the **IP Address** text box.
3. Select the AxTraxNG™ server's PC Port from the **Port** select box.
4. Click **OK**.

   The Server connection dialog box closes and the *Logon AxTraxNG™ Client* dialog box appears.



5. Select an **Operator name** and enter a **Password**.

Note

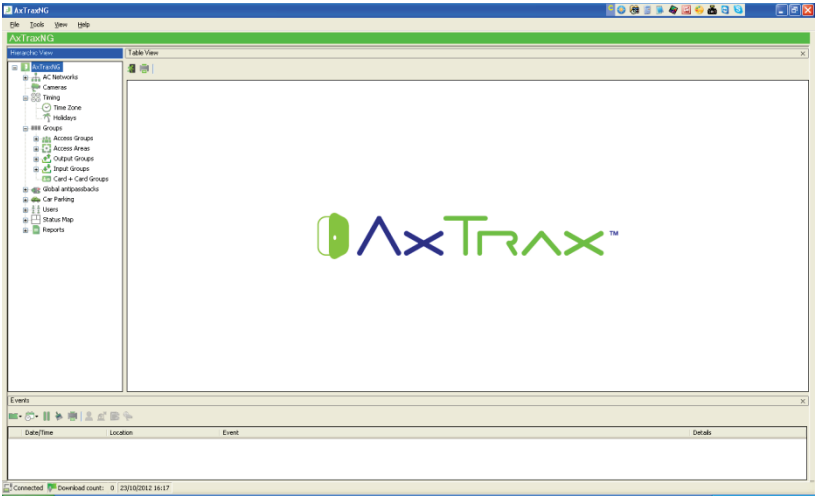
By default, the Administrator operator password is "admin".

6. Click **OK**.

   The main AxTraxNG™ window opens.

4.2 AxTraxNG™ Main Window

The entire central functionality of the AxTraxNG™ system is available from the AxTraxNG™ Client main window.



The AxTraxNG™ Client Main window is divided into six adjustable sections:

Table 1: AxTraxNG™ Client Main Window

Section		Description
1	**Menu Bar**	The Menu bar controls the software's general operation and setup. For more information, see Section 4.3.
2	**Toolbar**	The main Toolbar consists of icons for the key tasks required in managing access control across a facility. The available icons change according to the view selected. For more information, see Section 4.4.
3	**Tree View**	The Tree View allows users to configure, monitor, and control every aspect of access control. For more information, see Section 4.5.

Section		Description
4	**Event Log**	The Event Log displays a detailed log of every time access was granted or denied for every door on the site, as well as when inputs and output are opened or closed. The event log toolbar consists of icons allowing the user to monitor potential door tamper or forced entry attempts. These warnings are logged and displayed as internal system warnings, including video stream archives that are saved to the ViTrax™ database.
5	**Display Area**	The Display area displays all items within the selected Tree View element. It also provides options to add, edit, or delete items manually without opening the detailed element windows. In addition, the display area provides various system updates.
6	**Status Bar**	The Status Bar displays server connection status, Downloads Counter, and the Firmware programming progress bar.

4.3 Menu Bar

The menu bar controls the general operation and setup of the software.

4.3.1 File Menu

The File menu has three options:

Menu	Select Menu item to...
Server Connection	Log on to the AxTraxNG™ server
ViTrax Server	Log on to the ViTrax™ server
Exit	Exit the AxTraxNG™ software

4.3.2 Tools Menu

Use the Tools menu to manage the database and set software preferences. The menu has three options:

Menu	Select Menu item to...
Database	Open the Database window to back up the database or set a scheduled backup, as well as to import or export the AxTraxNG™ and/or VeriTrax AS-225/AxTrax AS-525 configuration states and events logs
Options	Set software options and preferences, including national holidays, event highlighting, custom user information fields, and GUI language
Import/Export Data	Import/export user information from/to an Excel spreadsheet file.

4.3.3 View Menu

Use the View menu to define and manage the view of the GUI. The menu has four options:

Menu	Select Menu item to...
Events	Select the option to show event logs
Table View	Select the option to show a detailed table view
Restore Docking	Restore the default GUI view
Close All Floating Windows	Close all pop-up windows at once

4.3.4 Help Menu

The help menu has one option:

Menu	Select menu item to...
About	View software, firmware, and database version information, as well as the current operator

4.4 Toolbar

The toolbar controls key tasks required to manage access control across an entire facility. When a new element is selected from the Tree View, the toolbar icons change to suit the selected element.

The following toolbar icons are available:

4.4.1 General Icons

Icon	Name	Click icon to...
	Manual Door Operation	Open the *Door Manual Operation* window (see Section 7.1)
	Print	Send the current display area view to the printer
	Add	Add a new element of the selected type
	Edit	Edit the selected element
	Delete	Delete the selected item
	Reader Type	Configure custom reader type

4.4.2 General Network Icons

Icon	Name	Click icon to...
	Add to Status Map	Add available panels and panel components to the Status Map (see Section 4.5.7)
	Download Failed Data Manually	Download the entire panels' failed database (see Section 9.2)

4.4.3 Network Icons

Icon	Name	Click icon to...
	Set Time	Set the time on the selected access control panel (see Section 9.1)
	Find Panels	Find and update panels within the network (see Section 5.4.2)
	Manual Modem	Open the *Modem Status* window to allow the operator to connect or disconnect the modem and change the connection password (see Appendix C)
	Camera	View a list of connected cameras, and assign the cameras to panels (see Section 6.2)

4.4.4 Panel Icons

Icon	Name	Click icon to...
	Manual Reader	Change the operation mode of the readers on the selected panel (see Section 7.2)
	Update Firmware	Send a firmware update to the selected access control panel (see Section 7.6)
	Control Output Manually	Change the settings for the outputs on the selected panel (see Section 7.3)
	Control Input Manually	Change the settings for the inputs on the selected panel (see Section 7.4)
	Control Siren Manually	Test the siren for the selected panel (see Section 7.5)

4.4.5 Card\Users Icons

Icon	Name	Click icon to...
	User Counter	View the current user count value (see Section 9.3)
	Add users	Create up to 1000 new users in one click (Section 0)
	Add cards	Create up to 1000 new cards in one click (Section 0)
	Assign cards	Add and assign cards to selected users or add cards from MD-08 (see Appendix G)
	User Filter	Filter the list of users by various parameters, such as name and card number (see Section 4.5.6.3)

4.4.6 Reports Icons

Icon	Name	Click icon to...
	Produce Report	Produce the selected report (Chapter 8)
	Print	Send the current report to the printer
	View Last Hour Access	Display relevant access events that occurred within the last hour (Chapter 8) **Note: This icon appears only when a Roll Call – Readers report is selected.**
	View Periodic Access	Displays relevant access events that occurred within a selected time frame (Chapter 8) **Note: This icon appears only when a Roll Call – Readers report is selected.**

4.4.7 Events Toolbar Icons

When clicking an event icon, click the dropdown arrow to change the current view of the display.

Icon	Name	Click icon to...
	Panel	Display all event types uploaded from the access control units
	Access	Display only access events uploaded from access control units
	Alarm	Display only alarm events uploaded from access control units

Icon	Name	Click icon to...
	Archive	Display video stream archive events stored in either the ViTrax™ database, the USB key, or snapshots saved on PC
	System	Display events related to the AxTraxNG™ Server operation and operators activity
	Pause	Halt the display of events in the display area. New events are shown again when the Pause button is clicked a second time.
	Refresh	Manually refresh the event list
	View Events within the last Hour	Display all events that occurred within the last hour. Click the dropdown arrow to change the view.
	View Events within the last Day	Display all events that occurred within the last day
	View Events within the last Week	Display all events that occurred within the last week
	View Periodical Events	Display all events that occurred within a selected period
	View All Events	Display all events
	Clear	Clear the entire log and empty the current event list view
	Show User	Open the *User* window for the selected user.
	Clear Alarm	Open the *Alarm Details* window to allow the operator to reset the alarm.
	Antipassback Forgive	Open the *Antipassback Forgive* window to allow the operator to cancel an Antipassback restriction for the selected user.
	Camera List	Open a list of all ViTrax™ cameras attached to the network
	Archive	Open the *Archive Camera* window for the selected video stream or snapshot.
	Car Parking	Opens the *Car Parking Counters* window to view and edit the car parking area and group counters.

4.5 Tree View

The Tree View allows users to configure, monitor, and control every aspect of a facility's access control network.

When the user selects an element from the Tree View, its contents are shown in the main display area, and the toolbar icons change to suit the selected element.

4.5.1 AC Networks

A network is a group of up to 32 access control panels. The AxTraxNG™ Server connects to the panels across the panel network.

For more information, see Section 5.3.

4.5.2 Cameras

Cameras can be added to the network to allow real-time viewing of any area desired. The **Camera** element allows you to add cameras to the network and to configure each camera's setting.

For more information, see Section 5.8.

4.5.3 Timing

The Timing tree branch consists of two elements: time zones and Holidays.

4.5.3.1 Time Zones

A time zone defines a weekly time period or set of time periods; for example, "Office Hours" or "Out of Office Hours". Door access rights, alarms, and input and output behavior can all be set to behave differently within each Time Zone.

For more information, see Section 5.1.

4.5.3.2 Holidays

This element defines annual holiday dates; it is possible to set special access behaviors for holiday time.

For more information, see Section 5.2.

4.5.4 Groups

The **Groups** tree branch consists of four elements: **Access groups**, **Access Areas, Output Groups,** and **Input Groups**.

4.5.4.1 Access Groups

An Access Group defines when each reader on the site is available for access. All site personnel are assigned to appropriate Access Groups.

For more information, see Section 5.10.1.

4.5.4.2 Input and Output Groups

Input and Output groups define sets of outputs or inputs that should be managed together within a panel.

For more information, see Sections 5.10.1, 5.10.2, and 5.10.3.

4.5.4.3 Access Areas

A facility can be subdivided into several access areas to configure and manage it more effectively.

For more information, see Section 5.13.

4.5.5 Global Antipassback

Antipassback rules can be applied to each access area to prevent one user's card or entry code from being used for two subsequent entries, and to prevent a second entry without a previous exit.

For more information, see Section 5.14.

4.5.6 Users

The **Users** tree branch consists of five elements: **Departments/Users**, **Visitors**, **User Filter**, **Cards**, and **Operators**.

4.5.6.1 Departments/Users

This element shows a list of all departments and users, as well as any visitors registered in the system. Each user is a member of a department. For each user, it is possible to assign cards and/or a PIN code, set access rights, personal details, and include an identification photograph.

For more information, see Section 2.

4.5.6.2 Visitors

This element shows a list of all visitors registered in the system.

Visitor type users can also be created with specific access rights.

For more information, see Section 2.

4.5.6.3 User Filter

This element allows you to find users in the database based on various search parameters, such as name, user number, and access group. The filtered list then appears in the main window.

4.5.6.4 Cards

This element lists all cards in the system with their statuses, and allows the manual or automatic addition of cards to the system.

For more information, see Section 5.10.4.2.

4.5.6.5 Operators

Operators are people with access to the AxTraxNG™ software. The default operator names are Administrator, Engineer, and Security.

Different operators have wider or more restricted security rights, from complete control over the system to the ability only to view one section. All Operator passwords are case-sensitive.

For more information, see Section 5.16.

4.5.7 Status Map

The Status Map creates a graphic display of the statuses for every door, reader, and alarm in the facility on user-selected images.

The system can display multiple nested status maps, allowing users to show either the complete access control network or a specific area in detail. For more information, see Section 5.18.

4.5.8 Reports

AxTraxNG™ can produce various reports, including usage reports, attendance records, visitors, and roll calls. The AxTraxNG™ Report Wizard allows users to design their own custom reports based on their needs. For more information, see Chapter 8.

5. How to Set Up a Site

This section outlines a recommended step-by-step process for configuring AxTraxNG™ for a site.

Step	Action	Section
1	**Add Time Zones and Holidays**	5.1 and 5.2
2	**Add a Network**	5.3
3	**Add and Configure an Access Control Panel**	5.4
4	**Configure the Doors**	5.5
5	**Configure the Readers**	5.6
6	**Configure the Inputs**	0
7	**Add a Camera**	5.8
8	**Add Panel Links**	5.9
9	**Create Groups: Access Groups, Input Groups, and Output Groups**	5.10.1, 5.10.2, and 5.10.3
10	**Add New Users and Cards**	5.11
11	**Add Departments, Users and Visitors**	2
12	**Add Access Areas and Add Global Antipassback Rules**	5.13 and 5.14
13	**Add Car Parking**	5.15
14	**Add Operator**	iv
15	**Add a Status Map**	5.18

The AxTraxNG™ system performs an automatic data download for any parameter related to the hardware. If panels are connected and active, a download count appears on the status bar after any downloaded parameter change. The counter shows **"0"** when a download is complete; however, it may also appear after a failed download.

It is the operator's responsibility to verify that the download operation succeeded or failed. This can be verified in the system event list or by checking the failed download data manually (see Section 9.2).

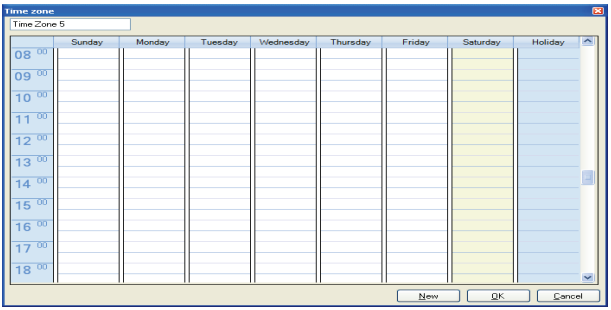
5.1 Adding Time Zones

A time zone is a group of periods within a week. Door access rights, as well as alarms and input and output behavior, can all be set to behave differently for each time zone. Many operations can be automatically enabled or disabled within a selected time zone.

The *Time Zone Properties* window displays the selected periods for each day of the week. It is possible to set a maximum of eight different time zone periods.

To add a new time zone:

1. In the Tree View, select **Timing > Time Zone**.
2. Click the icon on the toolbar.
   The Add *Time Zone* properties window opens.



3. Enter a name for the time zone.
4. Click and drag the mouse down a day column to select a time interval.
5. Right-click the selected area and select **Create**.
6. Right-click the selected area and select **Properties** to fine tune the time frame and then click **OK**.
7. Repeat Steps 4 to 6 for each day.

Note
You can move a defined time zone to a different day and time using drag and drop.

8. Click **OK** when all of the time zones are defined.

Note
You can create up to 8 time intervals for each day.

5.2 Adding Holidays

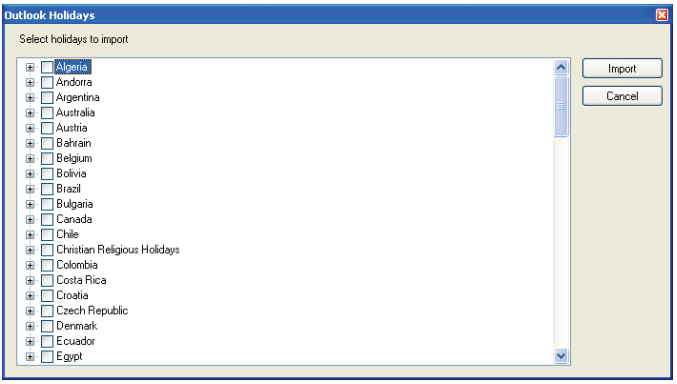
You can add and define annual holiday dates on which it is then possible to set special access behaviors.

There are two ways to add holidays:

- Add a known national holiday(s)
- Add a new holiday

To add a national holiday:

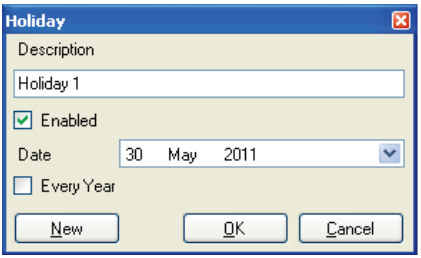
1. In the Tree View, select the **Holidays** element.
2. Click the icon.
   The *Outlook Holidays* window opens.



3. From the list, find the relevant country and either:
   a. Select the main checkbox to select all holidays for that country.
   b. Expand the checkbox and choose which holidays to add.
4. Click **Import**.
5. Click **OK** to confirm.
6. Click **OK** to close the *Options* window.

To add a new holiday:

1. In the Tree View, select **Timing > Holiday**.
2. Click the icon on the toolbar.
   The *Add Holiday* window opens.



3. In **Description**, enter a name for the holiday.
4. Select the **Enabled** checkbox to enable the holiday.
5. Use the **Date** dropdown to select the holiday's date.
6. Select the **Every Year** checkbox to repeat the date yearly.
7. Click **OK**.

5.3 Adding a Network

A network is a group of up to 32 access control panels. AxTraxNG™ communicates with each access control panel that is part of the network.

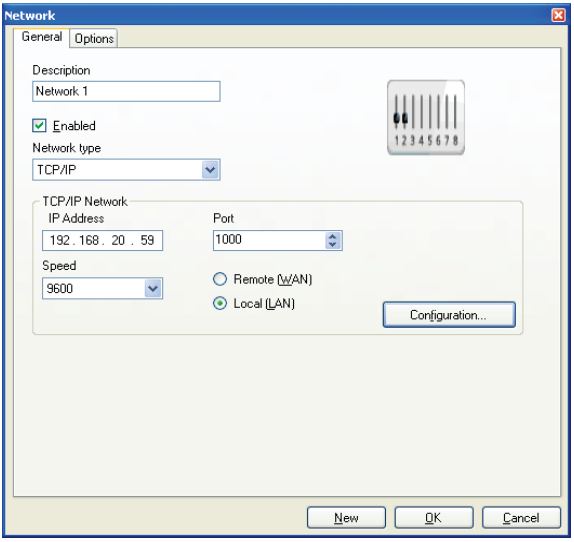
The *Network* window includes the following information:

- The network's name, address, and activation status
- The DIP switch settings for the communication speed
- The type of network connection and the connection settings

To add a network:

1. In the Tree view, select *Networks*.
2. Expand the **Networks** element to view available networks.

3. On the *Network* toolbar, click the icon.
   The Add *Network* window opens.



The *General* tab contains the following fields:

Table 2: Add Network > Options Tab

Field	Description
Description	Name for the network The network address appears to the right of the network name.
Enabled	Checkbox is selected when the network is connected and operational.

Field	Description
Network Type	Network type: *Serial*, *TCP/IP*, or *Modem* For TCP/IP connection, set the TCP/IP network (see Appendix C).
Configuration Button	Configuration window to set communication preferences. This button appears when selecting a Modem or TCP/IP LAN network. For more information, see Appendix C.

4. In **Description**, enter a name for the new network.
5. Select the **Enabled** checkbox.
6. In **Network type**, select the network type and set the connection settings:
   a. For serial, select the correct COM port.
   b. For a TCP/IP LAN, click **Configuration** to locate the hardware on the local network.
   c. For a modem, click **Configuration** to set dialing preferences for the computer's and the receiving modems.

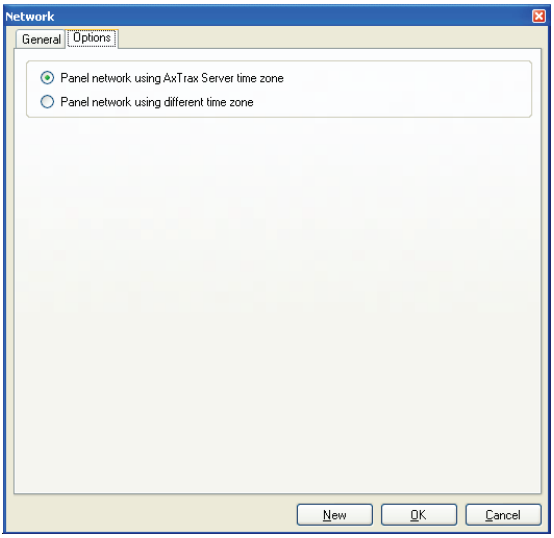
   For more information on how to configure an access control network, see Appendix C. Check with your system administrator for more information, or contact Rosslare technical support. Clear the *Enabled* checkbox if you want to halt communication to panels on the network.

Access control panels connect to a TCP/IP network via MD-N32 TCP/IP to a serial converter, or by using the on-board module in AC-225IP, AC-425IP, or AC-525. Refer to the relevant hardware installation guides for more details.

7. For all types of networks, set the DIP switch on the access control panel hardware to match the diagram at the top of the screen.

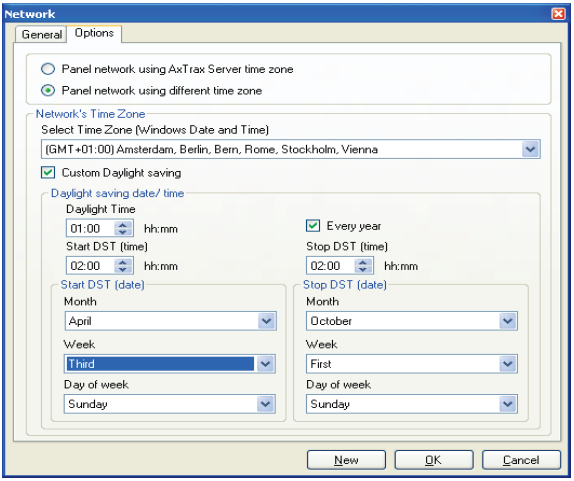
After changing the DIP switch, make sure to power down and then power up the panels.

8. In the Add *Network* window, click the *Options* tab.



9. To use the time zone of the AxTraxNG™ Server for the panel network, select **Panel network using AxTraxNG™ Server time zone** (default), and then continue to Step 12.
10. To select a different time zone for the panel network, select **Panel network using different time zone**.

    The Network Time Zone area opens.



The Network Time Zone area contains the following fields:

Table 3: Add Network > Options Tab

Field	Description
Select Time Zone (Windows Date and Time)	From the dropdown list, select the desired time zone.
Custom Daylight saving	Select the checkbox to define custom settings.
Daylight Time	Select the new hour at the time that daylight saving time begins.
Start DST (time)	Select the hour that daylight saving time begins.
Stop DST (time)	Select the hour that daylight saving time ends.
Every year	Select the **Every year** checkbox to set a day in one of the weeks of a defined month to automatically begin and end daylight saving time every year. Clear the **Every year** checkbox to set a date for one-time setting of the beginning and end of daylight saving time. In this case, a new date must be set each year.
Start DST (date)	If **Every year** is not selected, select the commence date for daylight saving time.
Month, Week, Day of Week	These fields are enabled when the **Every year** checkbox is selected. Select the month, week within the month, and day of the week when daylight saving time is to begin every year.
Stop DST (date)	If **Every year** is not selected, select the end date for daylight saving time.
Month, Week, Day of Week	These fields are enabled when the **Every year** checkbox is selected. Select the month, week within the month, and day of the week when daylight saving time is to end every year.

11. Set the Daylight Saving Time definitions according to the field descriptions in the table.
12. Click **New** from within Network tab to add a new network.
13. Click **OK** to exit the *Network's Time Zone* setup window.

5.4 Adding Access Control Panels

Every network is a cluster of access control panels. In its standard form, each access control panel can be configured as either one or two readers per door. Each of the AC-215, AC-225, and AC-525 panels have two readers and can be configured as a one or two-door panel. Each AC-425 panel has four readers and can be configured as a two or four-door panel.

When using an optional MD-D02 (supported by AC-225 or AC-525) or MD-D04 (supported by the AC-425) reader expansion board, each panel has four or eight readers and is configurable as such.

Use two readers per door when one door acts as both the entrance and exit to an area of the site. When only an entry reader is required, use one reader per door.

For example:

- Use configuration with two readers per door set to IN and OUT to produce attendance reports.
- Use one reader per door configuration to control two doors with an IN reader only (premises will be exited using a REX switch or a mechanical door handle only).

When there is communication with the panel, the Tx and Rx LEDs flash.

5.4.1 General Panel Settings

The *General* tab of the Door Controller Panel Properties window displays the following:

- The panel's address and status
- The DIP switch settings for the panel

If panel expansion boards are installed, the tab also displays:

- The input and output connections for the panel
- The panel's hardware version

Refer to AC-525 Hardware manual for further details.

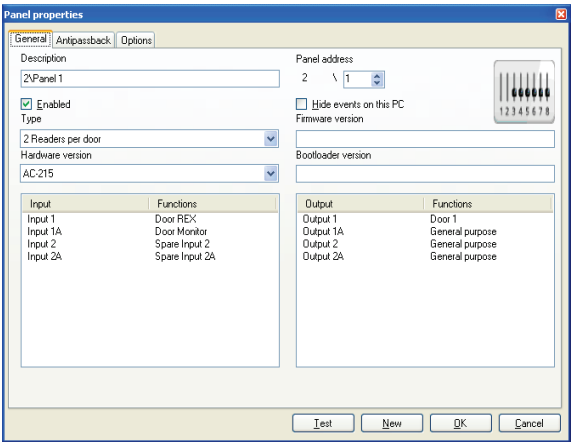
5.4.2 Adding a Panel

You can add an individual panel using the Tree View.

Alternatively, it is possible to search for panels over the access control network using the *Find Panels* option. This is particularly useful during installations. AxTraxNG™ finds all connected panels in the network and checks them. Panels can then be quickly activated and updated.

To add an individual panel:

1. In the Tree View, click **AC Networks**.
2. Select an available network.
3. On the toolbar, click the icon.
   The *Add Panel* window opens.



The *General* tab of the Door Controller *Panel properties* window contains the following fields:

Table 4: Door Controller>Panel Properties>General Tab

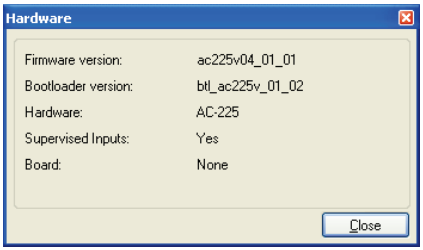
Field	Description
Description	Type a description for the panel
Panel Address	Type an address number for the panel The network's address appears to the left of the panel address. Valid entries are 1-32.
Enabled	Select the checkbox to activate this panel Clear the checkbox if the panel is not connected
Hide events on this PC	Select the checkbox to hide events originating from this PC
Type	Select one or two readers per door
Hardware Version	Select the appropriate panel hardware type
Firmware version	Upon selection of the hardware version, the field displays the current firmware version
Boot loader version	Upon selection of the hardware version, the field displays the current boot loader version
Inputs	Displays the input connections for the panel
Outputs	Displays the output connections for the panel
Test	Click to test if that the panel is correctly connected to the computer The Test Panel window displays hardware details, including hardware type, firmware, and boot loader versions, and indicates whether a reader or I/O expansion board is installed on the panel.

Note

Make sure that the DIP Switch 3 position on the panel corresponds with its position demonstrated in the *Panel properties* window.

4. Click **Test**.

   The *Hardware Test* window opens with the complete panel details.



The test screen displays the following information:

Field	Description
Firmware version	Displays the firmware version of the board
Bootloader version	Displays the boot loader version of the board
Hardware	Displays the hardware name
Supervised Inputs	Displays the panel is secure in case of tampering
MD-IO84	Indicates whether or not MD-IO84 exists
MD-D02	Indicates whether or not MD-D02 exists
MD-D04	Indicates whether or not MD-D04 exists
MD-IPAV1	Displays the AC-525 Video board version number

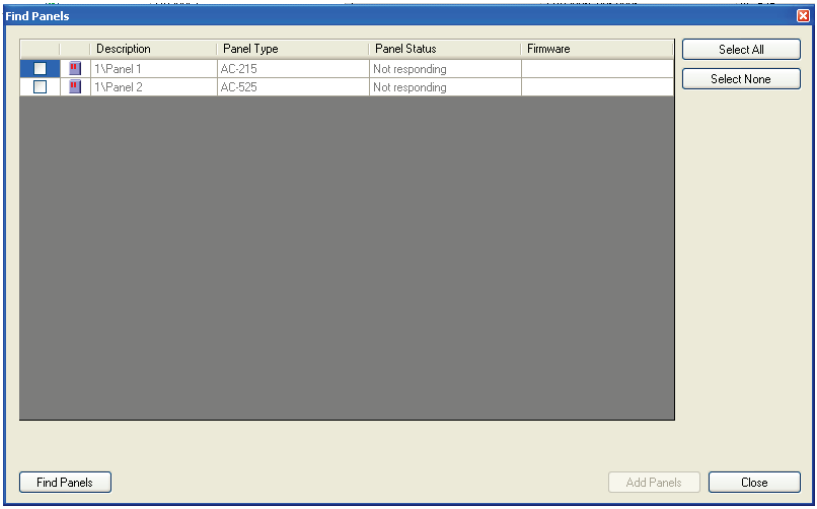
5. Click **Close**.

   The window closes and the display area displays the newly configured panel.

To search for existing panel on the network:

1. In the Tree View, expand the **AC Networks** element and select a network.
2. Click the icon.

   The Find Panels window opens.



3. Click **Find Panels** to search for all connected panels in the network.

   Once the detection process is complete (this may take 2-3 minutes), the display shows all of the detected panels and their corresponding information.

4. Select the panels that you wish to activate and click **Add Panels**.

   The selected panels then automatically appear in the Tree View under current network.

5.4.3 Editing the Panel

Each panel has individual settings for antipassback behavior and for recording events.

Once the panel is connected, edit the panel's options from the *Antipassback* and *Options* tabs in the *Panel properties* window.

The Antipassback tab contains the following fields:

Table 5: Network > Panel Properties > Antipassback Tab

Field	Description
Automatic Antipassback	From the *Automatic Antipassback* dropdown menu, select the time zone for door Antipassback rules to apply.
Antipassback severity	Choose the antipassback severity: • **Hard** – When hard Antipassback is selected, an event is generated and the door does not open. • **Soft** – When soft Antipassback is selected, an event is generated and the door opens.
In/Out reader list	From the IN/OUT readers list, select the checkboxes to apply Antipassback restrictions to Reader 1 through Reader 8, as required. The reader antipassback is enabled when the checkbox is selected.

The *Options* tab contains the following fields:

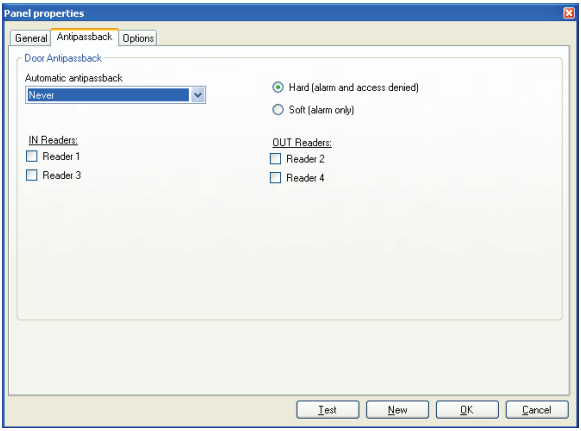
Table 6: Network > Panel Properties > Options Tab

Field	Description
Events filter	Click **Select** to open the Events Filter and select the events that this panel should record. Set the filter's operation method: • **Always Active –** Only the selected events are recorded by the panel • **Active when panel disconnected** – If the panel is disconnected from the AxTraxNG™ server, only the selected events are recorded. When the panel is connected to the server, all events are recorded. **Note: In the default configuration, some events are filtered and may not be seen in the display area Events view**
Door Interlock	Select the **Enabled** checkbox to enable Door Interlock. Select the **Door 1-8** checkboxes to apply the Door Interlock restrictions to Doors 1-8. The Door Interlock function is only enabled when the **Enable** checkboxes and a minimum of two doors are selected.
AC-525 USB Storage (applicable when connected to AC-525 only)	From the **Alarm Threshold Range (%)** dropdown menu, select the percentage of available memory consumed to determine when the system generates the "USB Disk Low Level" event. The USB disk on key status is monitored roughly once an hour. Therefore, be sure to select an acceptably low threshold level and consider that any related alarm may be set off up to one minute after the actual event occurs.

Field	Description
Full Upload	Click **Start** to re-upload all events from panel memory. Use the option only after consulting Rosslare's Technical Support. **Note: A full upload can take up to 3 hours.**
User Counter on re-enable the panel	This option allows you to reset the user counter to its starting value in the event that a panel is disconnected and then reconnected again. This option is only visible when the **Deduct User Counter** checkbox is selected in the *General* tab of the *Readers Properties* window (Section 5.6.1).

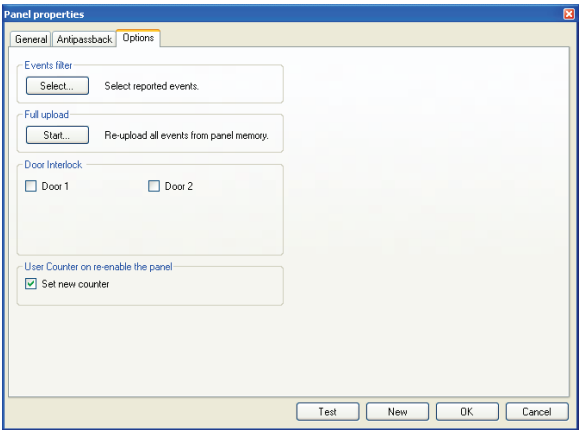
To edit a panel:

1. In the Tree View, click **AC Networks**.
   The available networks are listed in the display area.
2. Expand a network.
3. Click **Edit**.
   The *Panel Properties* window appears.
4. Click the *Antipassback* tab.



   Each panel has individual antipassback settings for door antipassback behavior.
5. Set the Antipassback behavior, according to the field descriptions in the table.

6. Click the *Options* tab.



7. Set the event filtering options for this panel.
8. Click **OK**.

   The window closes and the configured panel is displayed.

5.5 Configuring the Doors

Each panel controls one to eight doors. Each door can be configured individually.

The *Door Properties* window displays the following:

- The settings for unlocking and relocking
- The time available before the door relocks or records alarm events

The *Door Properties* window contains the following fields:

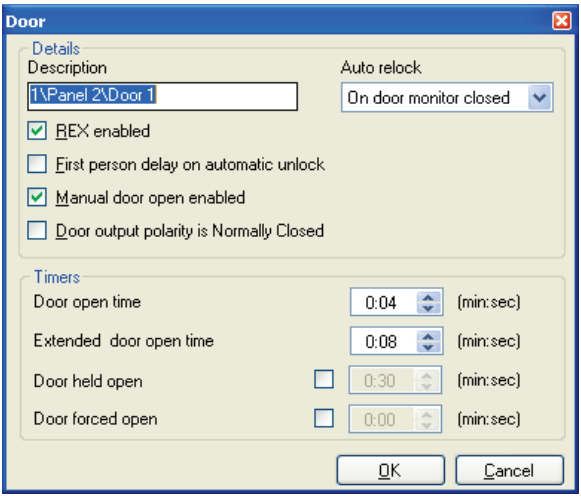
Table 7: Network > Panel > Doors > Door Properties

Field	Description
Description	Type a name for the door.
Auto-Relock	Select the event that causes the door to relock automatically.
REX enabled	A Request to Exit unlocks the door for a user-defined duration. Select the checkbox to allow Requests to Exit for this door. The location of the door REX input depends on panel configurations; it can be seen in the Panel properties window.
First person delay on automatic unlock	Sets the door's behavior during an automatic unlock time zone. Select the checkbox to require that during the selected Time Zone, the door remains locked until the first user opens it. The automatic unlock time zone is selected in Panel Links by selecting the output corresponding to that door (see Section 5.9).

Field	Description
Door output polarity is Normal Closed	Select this checkbox to ensure Fail Safe door opening if the Fail Safe door Lock Device power fails. Once enabled, the door output relay is activated when the door is closed and is deactivated when the door is open. In this configuration, the Fail Safe lock device should be wired to the door relay N.O. (Normal Open) and COM (Common) terminals.
Manual Door Open Enabled	Select this checkbox to allow operators to adjust the door manually (see Section 5.9).
Door open time	Set the duration for which the door stays unlocked.
Extended door open time	Set the duration for which the door stays unlocked for users with Extended door open rights.
Door held open	Set the duration for which the door can be held open without raising an alarm event. Select the checkbox to use this timer; for the Server application, the Pop-up and Snapshot section opens. **Note: If this feature is enabled, then the Activity start delay (Section 5.7) feature for that door must be set to 0.**
Door forced open	Set the duration after which when the door is forced open, an event occurs. Select the checkbox to use this timer; for the Server application, the Pop-up and Snapshot section opens. **Note: If this feature is enabled, then the Activity start delay (Section 5.7) feature for that door must be set to 0.**

To edit the door properties:

1. In the Tree View, click **AC Networks**.
2. Select a network and expand a panel in the Tree View.
3. Select **Doors**.
   The available doors are listed in the display area
4. Select a door in the display area and click **Edit**.
   The *Door Properties* window opens.



5. Configure the door as required.
6. Click **OK**.

5.6 Configuring the Readers

A panel can be connected to two, four, or eight readers, when the MD-D02 or MD-04 extension boards are connected.

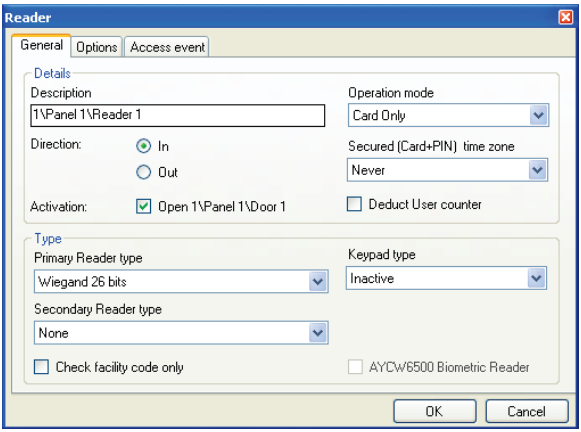
The *Reader Properties* window has three tabs:

- *General* tab – Sets the reader general operation settings
- *Options* tab – Sets access options for the reader
- *Access event* tab – Sets options for window pop-ups per event

5.6.1 General Tab

The *General* tab in the *Reader* window displays:

- The settings for how the reader operates
- The type of reader being used



The *General* tab in the *Reader* window contains the following:

Table 8: Network > Panel > Readers > Reader Properties > General Tab

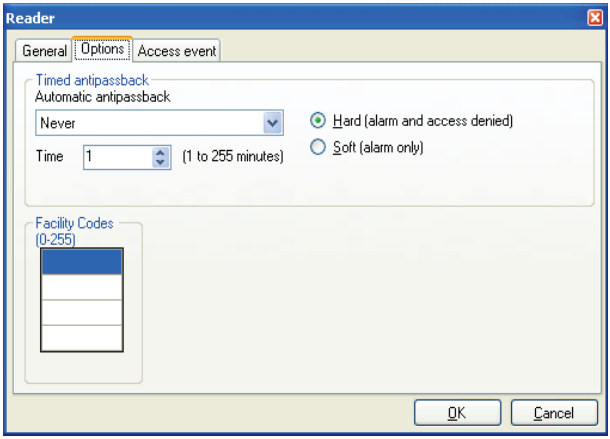
Field	Description
Description	Type the name of the reader.
Operation Mode	Select how the reader operates. • **Inactive:** The reader is not in use. • **Card Only:** The reader uses RFID cards only. • **PIN Only:** The reader uses PIN inputs only. • **Card or PIN:** The reader uses both cards and PIN codes. • **Desktop:** The reader is inactive, but is being used to record new cards on the computer. • **No Access Mode:** The reader does not grant access to any users.
Direction	Select whether the reader is allowing entry into the area or exit out of the area.
Secured (Card+PIN) time zone	Select a time zone during which access should be granted only after both the card and PIN are entered. The PIN must be entered within 10 seconds of card entry. **Note: When using a secured time zone, *Keypad type* must be defined.**
Open Door	Select the checkbox to allow the reader to unlock the door.
Deduct User Counter	Select the checkbox to record this entry against the user's entry allowance counter. See Section 5.12.2.1.
Primary Reader type	Select the data transmission type for the primary reader hardware.

Field	Description
Secondary Reader type	Select the data transmission type for the secondary reader hardware. **Note: This field is used when 2 different types of cards are used.**
Keypad type	Select the data transmission type for the type of keypad hardware.
Check facility code only	Select the checkbox to allow access to any user assigned to a facility listed in the selected list of facilities. The list of facilities is defined in the *Options* tab.
AYCW6500 Biometric Reader	Select the checkbox to interface with the AYC-W6500 biometric reader and its PC application, BioTrax.

5.6.2 Options Tab

The *Options* tab in the *Reader* window displays:

- Timed antipassback settings for the reader
- Restricted site access settings



The *Options* tab in the *Reader* window contains the following fields:

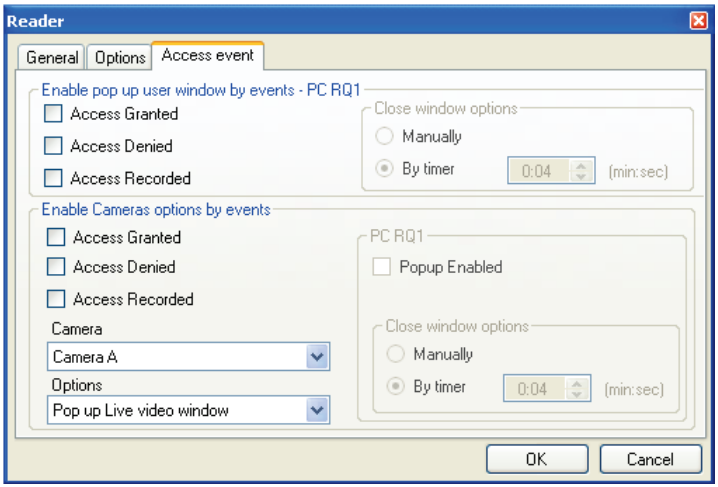
Table 9: Network > Panel > Readers > Reader Properties > Options Tab

Field	Description
Automatic Antipassback	Select whether to apply antipassback rules. To set Time Zones, see Section 5.1.
Hard	When hard antipassback is selected, an event is generated and the door does not open.
Soft	When soft antipassback is selected, the door opens but an event is generated.

Field	Description
Time	Set the number of minutes before a user can reenter using this reader.
Facility Codes	Click and type the facility code (between 0-255). Up to four different facility codes can be entered.

5.6.3 Access Event

The *Access event* tab in the *Reader* window defines the alerts pop-up windows behavior on the local PC.



It contains the following fields:

Table 10: Network > Panel > Readers > Reader Properties > Access Event Tab

Field	Description
Access Granted	Mark to checkbox to enable a pop-up window for Access Granted event type alerts.
Access Denied	Mark to checkbox to enable a pop-up window for Access Denied event type alerts.
Access Recorded	Mark to checkbox to enable a pop-up window for Access Recorded event type alerts.
Close window Options	Once a pop-up is enabled, the close window options are available. Select one of two options: • **Manually:** The operator is required to manually close the pop-up window. • **By timer:** The pop-up window closes automatically based on the predefined timer.

Field	Description
Camera **Available only with AC-525**	Select the name of the camera that takes snapshots or that appears when triggered by this reader. For example, the camera named 1\Panel 1\Camera A AC-525.

To configure a reader:

1. In the Tree View, click **AC Networks**.
2. Select a network and expand a panel in the Tree View.
3. Select **Readers.**

   The available readers are listed in the display area.
4. Select a reader in the display area and click the icon.

   The *Reader Properties* window opens to the *General* tab.
5. Configure the reader as needed using the tabs described in the above subsections.
6. Click **OK**.

5.7 Configuring the Inputs

Each panel has four inputs. Using the MD-IO84 expansion board adds an additional eight inputs (a total of 12 inputs). Using the MD-D02 or MD-D04 expansion board adds four inputs (a total of 8 inputs). Some inputs are dedicated and have default functionality and some are for general purpose.

The *Input Properties* table window displays the settings for each input. Input type is programmed individually, regardless of whether it is a dedicated input or for general purpose use.

The *Input Properties* table contains the following fields:

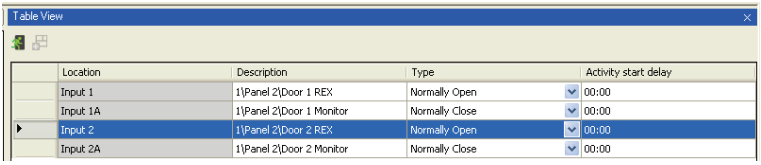
Table 11: Network > Panel > Inputs > Input Properties

Field	Description
Location	A display field showing the input name
Description	Type a name for the input.
Type	Select the type of input to be monitored. • **Normally Open/Close:** An input either in an open or closed state • **Normally Open/Close 1 Resistor:** An input in an open, closed, or trouble state. This option is only available for supervised inputs. • **Normally Open/Close 2 Resistors:** An input in an open, closed, or trouble state, with additional checks for short-circuit and open-circuit tampering. This option is only available for supervised inputs. For more information, refer to the Access Control Panel's hardware manual.

Field	Description
Activity start delay	Set the delay time before this input becomes active. Note that on normally open input, the delay starts once the input contact is closed. On normally closed input, the delay starts once the input contact opens.

To configure an input:

1. In the Tree View, click **AC Networks**.
2. Select a network and expand a panel in the Tree View.
3. Select **Inputs.**
   The available inputs are listed in the display area
4. Select an input from the display area and click **Edit**.
   The *Input Properties* window opens.



5. Select an input and configure it as required.

5.8 Adding a Camera

See Chapter 6.

5.9 Adding Panel Links

Panel links are rules defining how the system should behave when events occur in the access control panel.

The *Link Properties* window displays the following:

- An event on a panel and the panel component to which the link response applies
- The required input or output response
- Any alarm message to display on the current AxTraxNG™ Client computer

The *Add Link* window contains the following fields:

Table 12: Network > Panel > Links > Add Link Window

Field	Description
Source Type	Select the panel component type, input, output, reader, and so on which is the event source

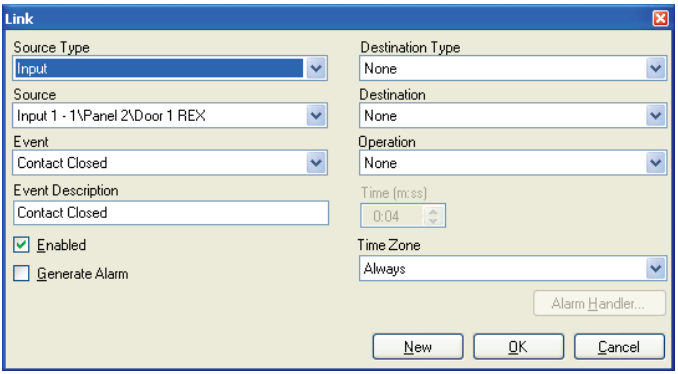
Field	Description
Source	Select the specific panel component that raises the event based on the source type selected. Up to 8 links can be created for each source type in the AC-225, AC-425, and AC-525 panels. Up to 2 links can be created for each source type in an AC-215 panel.
Event	Select the event type for the panel component
Event Description	Type the link or event description
Enabled	Select the checkbox to enable the link rule
Generate Alarm	Select the checkbox to generate an alarm event in addition to the link rule activity
Destination Type	Select the panel component type, which is to be activated by the link rule trigger event
Destination	Select the specific panel component, which is to be activated by the link rule trigger event
Operation	Select the operation performed by the destination panel component
Time	Define a duration timeframe for the operation. This box is only available when a time-bound operation is selected
Time Zone	Select the time zone for which the link rule applies
PTZ Preset position (available with AC-525)	Set the default preset PTZ (Pan, Tilt, Zoom) camera position **Note: To activate this feature, you must set the preset on ViTrax.**

Field	Description
Alarm Handler	Opens the Alarm Handler configuration window, which contains the following fields: • **Alarm Message:** Type a personalized message to be displayed on the screen as an alarm message when the selected event occurs • **Popup Enabled:** Select the checkbox to enable an alarm pop-up message • **Select Color button:** A color selection window opens allowing a color selection for the alarm message • **Browse… button:** Find and upload an audio wav file to be sounded when the selected event occurs • **Sound Now button:** After uploading the audio file click to button to hear the audio file • **Local Sound Enabled:** Select the checkbox to enable sound for the alarm • **Fire Input Alarm:** Select this checkbox to open all outputs, usually relevant for fire alarms The Alarm Handler function is only enabled when the *Generate Alarm* checkbox is selected. In addition, when a camera is linked to a panel, the following fields appear in the window: • **Camera**: List of available cameras • **Options**: How the alarm is displayed • **Popop Enabled**: Activates a popup to appear on the user's screen when alarm is triggered • **Close window options**: Can choose **By timer** and specify the time, or Manually

Numerous events and links can be defined in Panel Links. It is the operators' responsibility to avoid conflicting or non-logical definitions. Not all events sources that appear in the *Links* window are enabled in the panel; this too is the operator's responsibility to verify. Link condition operations should be checked after making any changes in the links definitions.

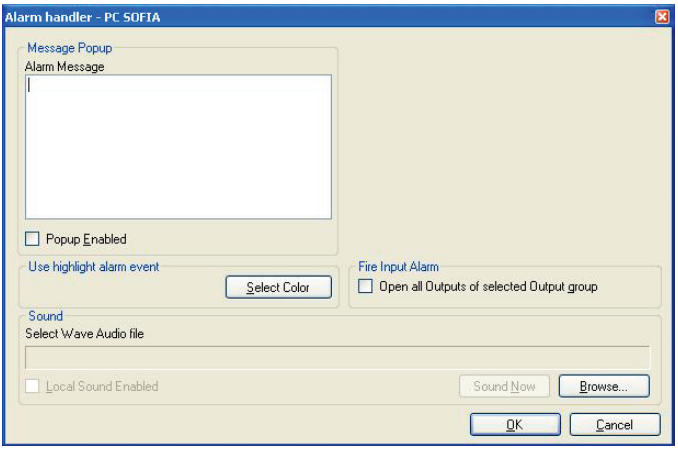
To create a panel link:

1. In the Tree View, click **AC Networks**.
2. Select a network and expand a panel in the Tree View.
3. Select **AC Links.**
4. On the *Network* toolbar, click the icon.
   The *Add Link* window opens.



5. Configure the link rule as required, according to the field descriptions in the table.
6. Select the **Generate Alarm** checkbox to activate the Alarm Handler button.
7. Click **Alarm Handler**.

   The *Alarm Handler* window opens.



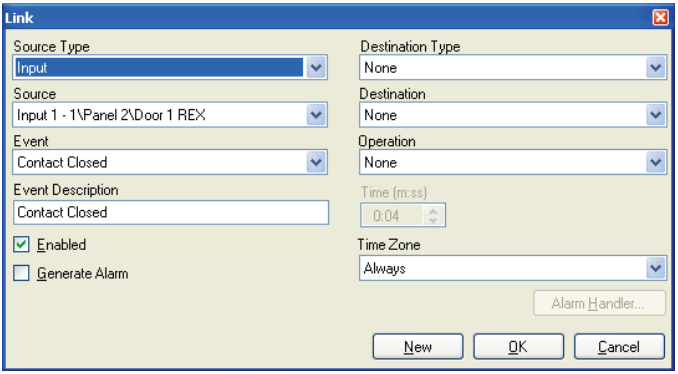
8. Configure the alarm handler as required, according to the field descriptions in the table above.
9. Click **OK** to close the *Alarm handler* window and return to the *Link* window.
10. Click **OK** to close the *Link* window and save the link rule configuration.

5.9.1 Creating a Fire Alarm Input

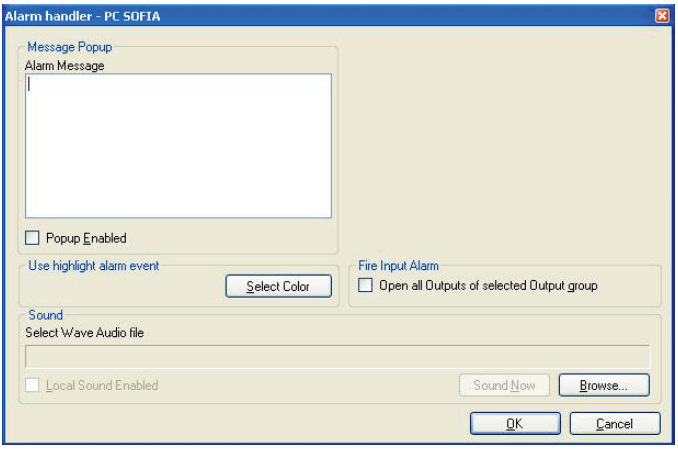
You can configure the panel properties to generate a fire alarm warning.

To create a fire alarm input:

1. In the Tree View, click **AC Networks**.
2. Select a network and expand a panel in the Tree View.
3. Select **AC Links.**
4. On the *Network* toolbar, click the icon.
   The *Add Link* window opens.



5. Configure the link as follows:
   a. In **Source Type**, select **Input**.
   b. In **Destination Type**, select **Output Group**.
   c. In **Operation**, select **Timer**.
   d. Select the **Generate Alarm** checkbox.
6. Click **Alarm Handler**.
   The *Alarm handler* window opens.



7. Configure the alarm handler as required, according to the field descriptions in the table above.
8. Select the **Open all Outputs of selected Output group** checkbox.
9. Click **OK** to close the *Alarm handler* window and return to the Add *Link* window.
10. Click **OK**.

5.10 Creating Groups

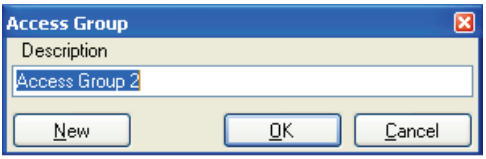
You can create access groups and areas, as well as input and output groups to be used by the system to create automated rules.

5.10.1 Adding Access Groups

An access group includes a list of door readers and the time zones during which each of those door readers are available for access. Every user is assigned to an access group.

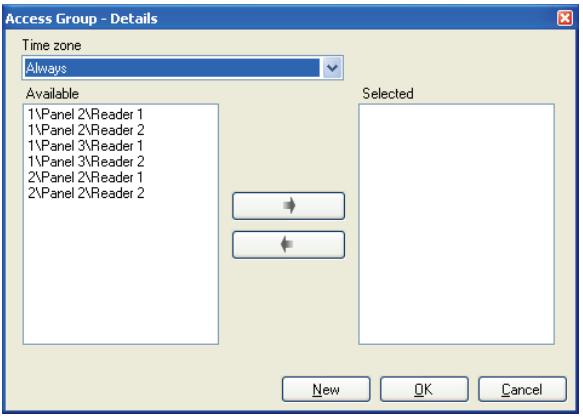
To add an access group:

1. In the Tree View, expand the *Groups* element and select **Access Groups**.
2. On the toolbar, click the icon.
   The *Add Access Group* window opens.



3. In the *Description* field, enter a name for the access group and click **OK**.
   The new access group appears in the View Tree.
4. Select the access group from the View Tree and click the icon.

The *Access Group Properties* window opens.



5. From the *Time zone* dropdown, select a time.
6. Select and move the desired readers from **Available** to **Selected** using the arrows.
7. Click **OK**.

   The window closes and the new access group appears in the Display Area.

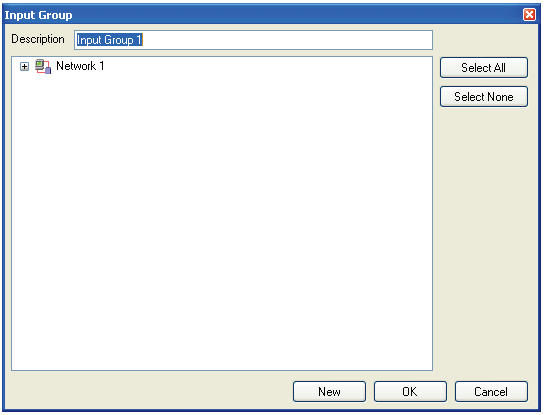
5.10.2 Adding Input Groups

Input groups are a collection of inputs from one or more panels that can be used in panel links to perform advanced operations.

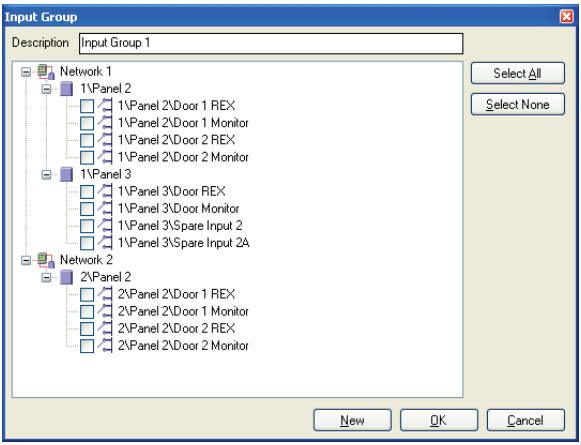
To create an input group:

1. In the Tree View, expand the ***Groups*** element.
2. Select **Inputs Groups** and click the icon.

   The *Input Group* window opens.



3. In the *Description* field, enter a name for the input group.
4. Expand a network to see its panels.



5. Select the checkboxes of all relevant inputs.

   You can also use **Select All** and **Select None**.
6. Click **OK**.

   The window closes and the new input group appears in the display area.

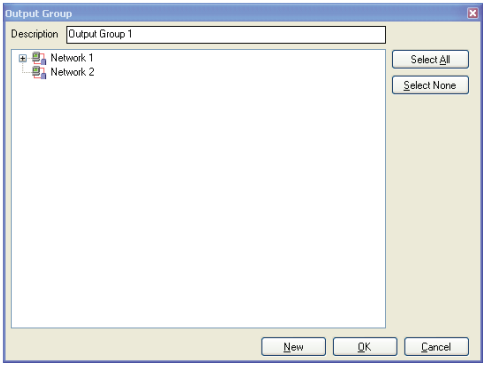
5.10.3 Adding Output Groups

Output groups are a collection of outputs from panel that can be used in panel links to perform advanced operations, such as elevator control.

To add an output group:

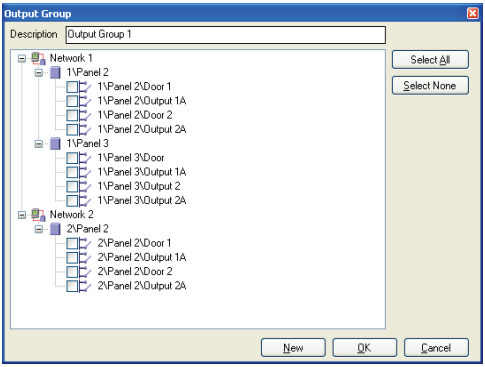
1. In the Tree View pane, expand the *Groups* element.
2. Select **Outputs Groups** and click the icon.

   The *Output Group* window opens.



3. In the **Description** field, enter a name for the input group.

4. Expand a network to see its panels.



5. Select the checkboxes of all relevant outputs.

   You can also use **Select All** and **Select None**.

6. Click **OK**.

   The window closes and the new output group appears in the display area.

5.10.4 Defining Card + Card Groups

Card + Card mode is a secure mode that requires two card holders (users) to grant access to a particular reader.

> Note
>
> This feature is only available to Access Control panels AC-225, AC-425, and AC-525.

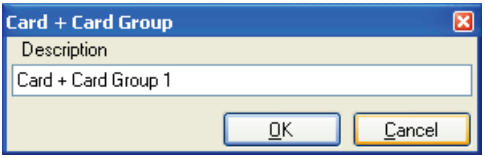
5.10.4.1 Adding a Card + Card Group

First, you must add a Card + Card group.

To add a Card + Card group:

1. In the Tree View pane, expand the *Groups* element.
2. Select **Card + Card Groups** and click the icon.

   The *Output Group* window opens.



3. In the **Description** field, enter a name for the input group.
4. Click **OK**.

   The window closes and the new Card + Card group appears in the display area.

5.10.4.2 Adding Users to a Card + Card Group

Once a Card + Card group is created, you must add users to it.

To add users to a Card + Card group:

1. In the Tree View, expand the **Departments/Users** element and select a department that contains the users you wish to add to the Card + Card group.
2. Select a user in the Table View area and click the icon.
3. In the General Tab of the User Properties window (see Section 5.12.2.1), select the Card + Card group from the **Card + Card Group** dropdown.
4. Click **OK**.
5. Repeat this process for each user you wish to add to a particular Card + Card group.

5.11 Adding Users and Cards

The AxTraxNG™ database maintains a list of every user card or PIN that has ever been assigned. The *Add Users and Cards* window is used to define:

- The type of reader needed to read the card
- The number of cards to create
- Whether or not a user should be created for each new card

The *Add Users and Cards* window contains the following fields:

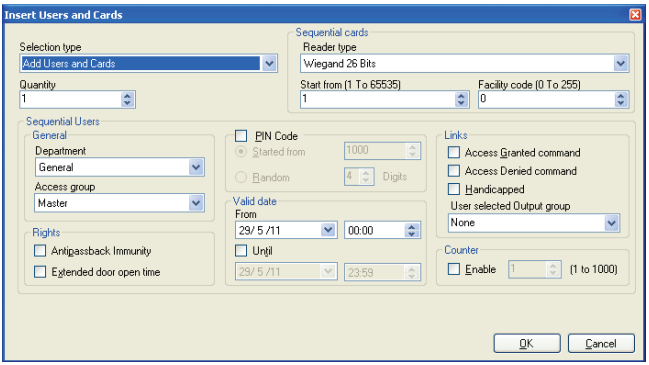
Table 13: Cards > Add Users and Cards Window

Field	Description
Selection Type	Select what will be added: Users and cards, Users only, or Cards only
Quantity	Type or select the number of cards/users to add
Sequential cards	Define the card properties: • **Reader Type:** Select the type of reader appropriate for the new cards being added • **Start from:** Type the number of the first card in the set • **Facility code:** Type the site code for these cards. This field is not available for all reader types
Sequential Users – General	Define the users general properties: • **Department:** Associate to the new user(s) created to a department • **Access Group:** Associate to the new user(s) created to an Access group

Field	Description
Sequential Users – Rights	Define the users right properties: • **Antipassback immunity:** Select the checkbox to override any antipassback restrictions • **Extended door open time:** Select the checkbox to activate the extended door option defined for each door
Sequential Users – Pin Code	Select the checkbox to define automatic pin codes, select between: • **Start from:** Sequential pin code starting from a predefined number based on a defined number of digits • **Random:** Random pin codes where the only definition is the number of PIN code digits
Sequential Users – Valid date	Define the access right validity: • **From:** Define the date and time to begin allowing access • **Until:** Select the checkbox to define an end date for the access right validity, then define the date and time
Sequential Users – Links	Select the checkbox to define associated link commands: • **Access Granted command:** Activate a user-defined set of inputs or outputs for access granted events • **Access Denied command:** Activate a user-defined set of inputs or outputs for access denied events • **Handicapped checkbox:** Activate a dedicated output a short time after the door is unlocked. The outputs are set in the Links window. • **User selected Output group:** Select an output group for this user. The outputs are triggered every time the user accesses a door. The operations, inputs, and outputs are defined in the Links window (see Section 5.9).
Sequential Users – Counter	Select the ***Enable*** checkbox to use the counter option then type or select the counter number to be used for the first user

To add users and cards:

1. In the Tree View, select **Cards**.
2. On the toolbar, click the icon.
   The *Add Users and Cards* window opens.



3. Configure the user and card properties as required, according to the field descriptions in the table above.
4. Click **OK** to close the window.

   The process may take a few minutes after which a dialog reports that the operation has been completed.

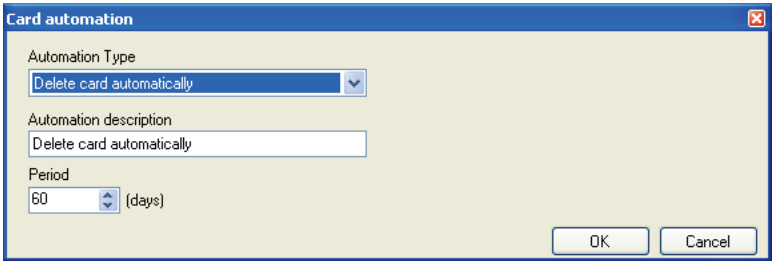
5.11.1 Setting Card Automation

You can program the system to automatically keep track of any user card that has expired because of non-use over specified period of time. Once detected, this card can either be deleted automatically or you can be notified of it.

To set card automation:

1. On the Tree View, expand the **Card** element and click **Card Automation**.

   The *Card automation* window opens.



2. From the **Automation Type** dropdown, choose the action to be taken when a card has not been used in a certain period of time.
   - Delete card automatically
   - Ask before card deletion
   - Notify by email
   - Report in System Event Log only
3. From the **Period** spin box, choose the time period.
4. Click **OK**.

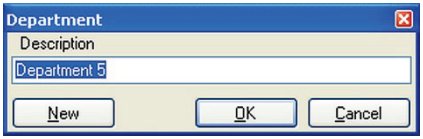
5.12 Adding Departments, Users, and Visitors

Every user is associated with a department. For each user, AxTraxNG™ stores contact details, associated card details, and access rights.

5.12.1 Adding Departments

To add a department:

1. In the Tree View, select the *Departments/Users* element.
2. To create a new department, click the icon.
   The Add *Department* window appears.



3. In the **Description** field, enter a name for the department and click **OK**.
   The window closes and a new department is created.

5.12.2 Adding Users

Adding users to a department is done by using the *Add User* window.

The *Add User* window contains three main tabs:

- *General* tab – Displays identification and control information
- *Codes* tab – Displays card information associated with the user
- *Details* tab – Records user contact details

In addition, there are two content-oriented windows:

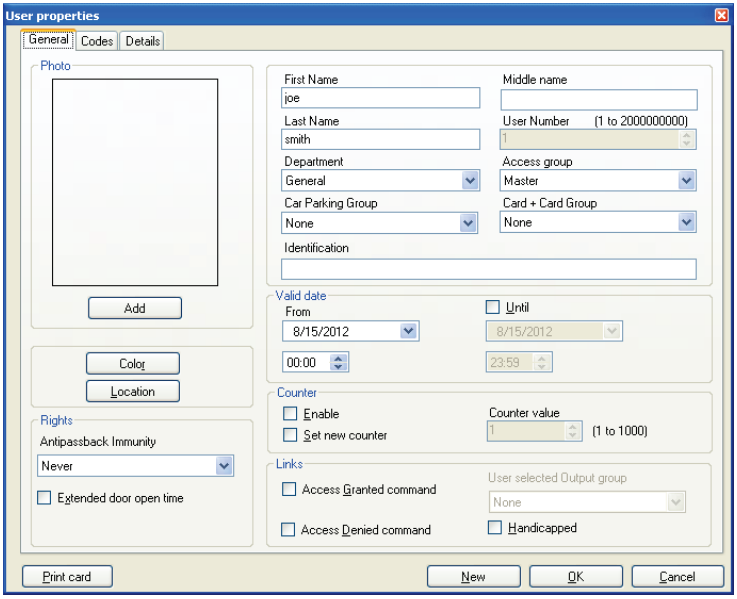
- *User Fields* – Stores user-defined data
- *Visitor* Tab – Appears when the user is defined as a visitor (Section 5.12.3)

5.12.2.1 General Tab

The General tab displays:

- User identification information
- User validity settings
- Access rights for the user

Figure 2: User Properties > General Tab



The *General* tab contains the following fields:

Table 14: Departments/Users > Department > User Properties > General Tab

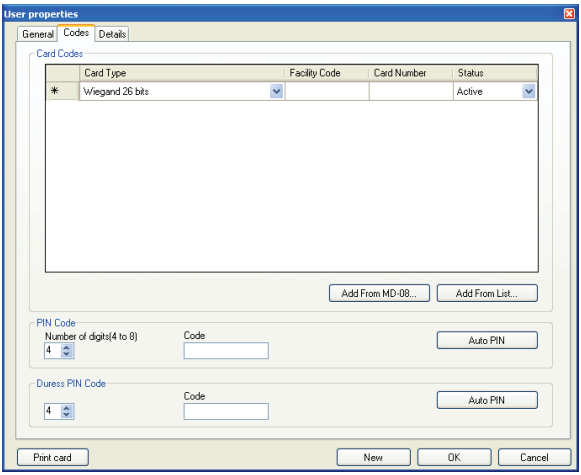
Field	Description
Photo > Add	Click to add a photo of the user, or to remove an existing photo. The selected photo aspect ratio should be 1.25 H x 1.00 L; otherwise, the photo may be distorted.
First name	Type the user's first name.
Middle name	Type the user's middle name.
Last name	Type the user's last name.
User number	Type a unique user number to identify the user.
Department	Select the user's associated department.
Access group	Select the user's access group.
Car Parking Group	Select to add a user to a defined Car Parking group.
Card + Card Group	Select to add a user to a defined Car + Card group.
Select color	Click to select which color to use to highlight this user when the user generates access events. User highlighting must be activated in **Tools > Options > General** tab.
Location	Click to display a log of doors accessed by this user.

Field	Description
Valid date > from	Select the date/time from when the user's access rights begin.
Valid date > until	Select the date/time on which the user's access rights end. This field is only available when the checkbox is selected.
Counter > Enable	Select the checkbox to set an access rights countdown counter for this user (see Appendix E). When the counter reaches zero, the user's access rights end.
Counter > Set new counter	Select the checkbox to set a new countdown counter value for this user (see Appendix E).
Counter > Counter Value	Select a new countdown counter value for this user. This field is only enabled when the *Set new counter* checkbox is selected.
Rights > Antipassback immunity	Select the checkbox to override any Antipassback restrictions for this user.
Rights > Extended door open time	Select the checkbox to entitle this user to an extended unlocked door duration. The extended duration is set for each door. See Section 5.5.
Links > Access Granted command	Select the checkbox to activate a link rule initiated by access granted commands for this user (see Section 5.9).
Links > Access Denied command	Select the checkbox to activate a link rule initiated by access denied commands for this user (see Section 5.9).
Links > User selected Output group	Select an output group for this user. The outputs are triggered every time the user accesses a door, as specified in the *Links* window (see Section 5.9).
Links > Handicapped check-box	Select the checkbox to activate a dedicated output a short time after the door is unlocked (see Section 5.9).

5.12.2.2 Codes Tab

The *Codes* tab displays:

- The cards assigned to this user (up to 16 cards)
- The PIN code assigned to this user



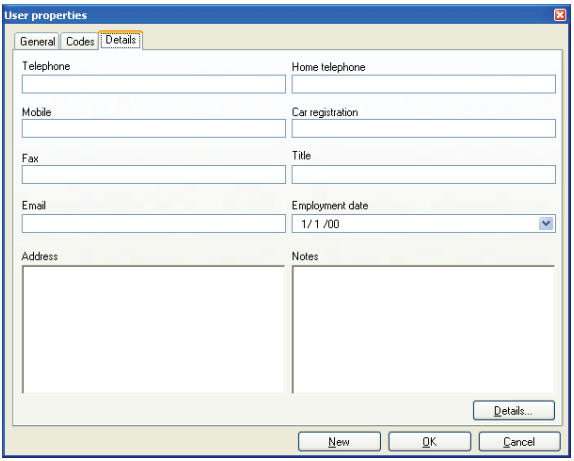
The *Codes* tab contains the following fields:

Table 15: Departments/Users > Department > User Properties > Codes Tab

Field	Description
Card Type	The card type used by the reader/user
Facility Code	The site code assigned to this card
Card Number	The unique number of this card
Status	Select the status of the card. Inactive cards cannot gain access to the facility
Number of digits	Select the length of the PIN for this user
Add from MD-D08	Click to read card details using MD-D08 module.
Add from list	Click to add a new card. All cards within the user's specified facility code, are listed
Code	The 4- to 8-digit PIN and/or Duress PIN code
Auto PIN	Click to automatically generate a random PIN

5.12.2.3 Details Tab

The *Details* tab contains detailed contact and identification details about the user.



The *Details* tab contains the following fields:

Table 16: Departments/Users > Department > User Properties > Details Tab

Field	Description
Telephone	Type an office telephone number for the user.
Mobile	Type a cell phone number for the user.
Fax	Type a fax number for the user.
Email	Type an email address for the user.
Address	Type a postal address for the user.
Home telephone	Type a home telephone number for the user.
Car registration	Type the user's license plate number.
Title	Type the user's title (e.g. "Mr.").
Employment Date	Enter the date that the user joined the firm.
Notes	Type any additional information.
Details	Click to open the user's additional details folder.

5.12.2.4 User Fields Tab

The User Fields tab can be used to store any information required by the system operator.

User fields are defined in the *Tools > Options > User Fields/Default* tab (see Section 9.5.2).

To add a user:

1. In the Tree View, expand the **Departments/Users** element and select a department for the new user.
2. On the toolbar, click the icon.

The *Add User* window opens.

3. Enter the user details as needed using the tabs described in the above subsections.
4. Click **OK**.

   The window closes and the added user is displayed.

5.12.3 Adding Visitors

AxTraxNG™ stores contact details for each visitor, associated card details, and visitor access rights.

The *Visitor's options* tab contains the following fields:

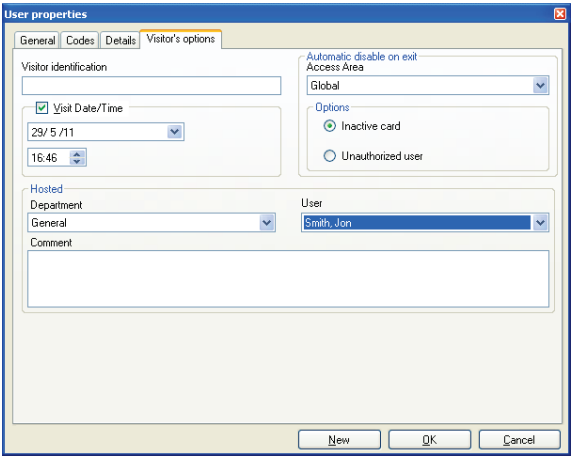
Table 17: Departments/Users > Visitors > Add User > Visitor's Options Tab

Field	Description
Visitor Identification	Type a unique visitor identification
Visit Date/Time	Select the checkbox and specify the date and time for the visit
Automatic disable on exit	Define automatic disable access right options • **Access Area:** Select the Access Area to disable access to • **Inactive card:** The designated card automatically becomes inactive upon exit • **Unauthorized user:** the designated access group changes to Unauthorized upon exit
Hosted	Define the details for the hosting party: • **Department:** Select the Department • **User:** Select the hosting User • **Comment:** Type any additional information

To create visitors:

1. In the Tree View, expand the *Users* element and select **Visitors**.
2. On the toolbar, click the icon.

   The same *Add User* window as before opens; however, now the *Visitor's Options* tab is available.



3. Enter the visitor specific options as needed.
4. Enter the visitor's details in the various tabs as explained in detail in the user subsections.
5. Click **OK**.

   The window closes and the added visitor is displayed.

Note

Users may be moved to other department or redefined as a Visitor. A visitor may be moved into any department and changed to a regular user. These can be done by using the General tab and selecting the new department to which you wish to the user or visitor.

5.13 Adding Access Areas

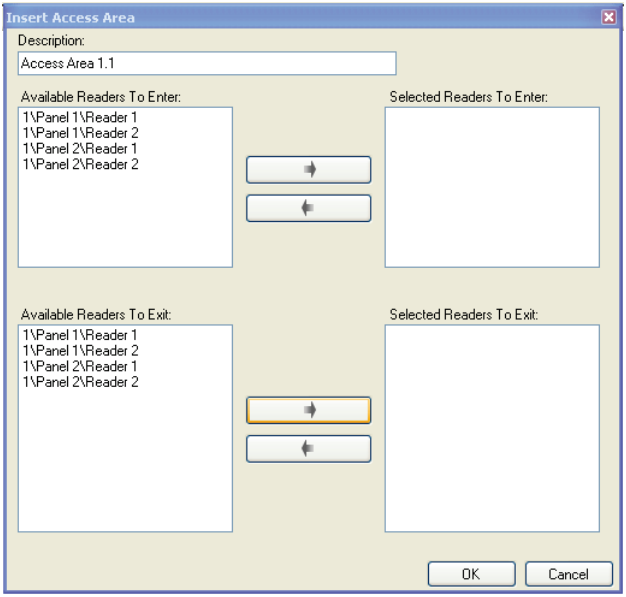
A large site can be divided into several smaller, more manageable access areas. Reports can be produced individually for each area. In addition, global Antipassback rules can be applied for each access area. When global Antipassback rules are in effect, users cannot re-enter an access area until they have left it.

Use the *Access Area* window to add entry and exit door readers to and from an area within the facility.

To add an access area:

1. In the Tree View, expand the **Groups** element.
2. Expand the **Access Areas** element and select **Global**.

3. On the toolbar, click the icon.
   The *Add Access Area* window opens.



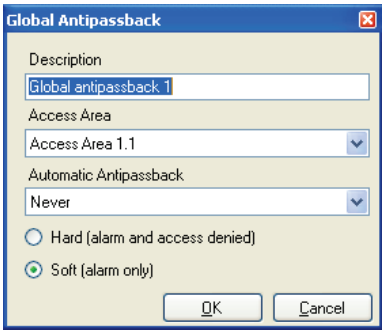
4. In the **Description** field, enter a name for the access area.
5. Select and move the desired readers from **Available Readers to Enter** to **Selected Readers to Enter** using the arrows.
6. Select and move the desired readers from **Available Readers to Exit** to **Selected Readers to Exit** using the arrows.
7. Click **OK**.
   The window closes and the new access areas appear in the Display Area.

5.14 Adding Global Antipassback Rules

Global antipassback functionality is only enforced when the AxTraxNG™ Server is connected and monitoring the entire access control system.

To create antipassback rules:

1. In the Tree View, select **Global Antipassback**.
2. On the toolbar, click the icon.
   The *Add Global Antipassback* window opens.



3. In the **Description** field, enter a name for the antipassback rule.
4. From the *Access Area* dropdown, select the access area.
5. From the *Automatic Antipassback* dropdown, select the time zone for which the global antipassback applies.
6. Select either the **Hard** or the **Soft** Antipassback option.
7. Click **OK**.

   The window closes and the global antipassback rule appears in the Display Area.

Note

Global Antipassback applies an Antipassback event only on "Enter" readers to the defined "Area".

To implement Antipassback on Exit readers as well, you must define a new area with opposite reader directions:

Readers defined "Enter" in the first area need to be defined again in the new area as "Exit" readers, and "Exit" readers in the first area should be defined as "Enter" readers in the second area.

5.15 Car Parking

The Car Parking management option allows you set up groups that have limited number of users who can access a particular area. For example, a parking lot that serves several companies and each company has a specified number of parking spots. With this option, we can set up each company's limit and when the limit is reached, access is no longer granted. This feature is counter based that keeps track of the number of users in a specified area.

Note

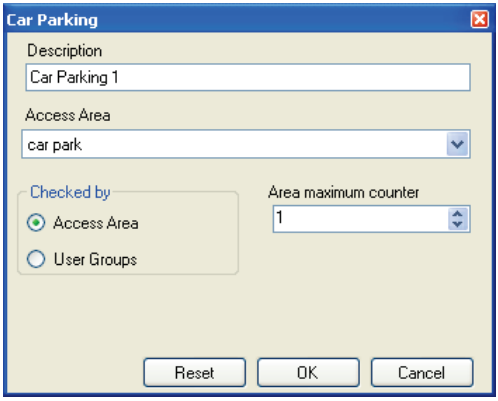
This feature is only available to Access Control panels AC-225, AC-425, and AC-525.

Note

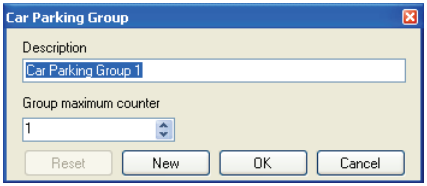
Only one car park area can be added per panel.

To define a car parking area:

1. Create an access area with Enter and Exit readers (see Section 5.13).
2. In the Tree View, select **Car Parking**.
3. On the toolbar, click the icon.
   The *Car Parking* window opens.



4. In **Description**, enter a name of the car parking element.
5. In **Access Area**, select the relevant access area that you defined in Step 1.
6. In the **Checked by** area, perform one of the following:
   a. Select **Access Area**.
      i. In **Area maximum counter**, choose the number of parking spots available in that access area.
      ii. Click **OK**.
   b. Select **User Groups**.
      i. Click **OK**.
      ii. In the Tree View, under **Car Parking**, choose the car parking area you just created.
      iii. On the toolbar, click the icon.
      The *Car Parking Group* window opens.



      iv. In **Description**, enter a name of the car parking sub-group.

v. In **Group maximum counter**, choose the number of parking spots available for the parking group.

vi. Click **OK**.

vii. In the Tree View, expand the **Departments/Users** element and select a department that contains the users you wish to add to the Car Parking sub-group.

viii. Select a user in the Table View area and click the icon.

ix. In the General Tab of the User Properties window (see Section 5.12.2.1), select the Car Parking sub-group from the **Car Parking Group** dropdown.

x. Click **OK**.

xi. Repeat Steps viii and ix for each user you wish to add to a particular Card + Card group.

xii. Repeat Steps iii to xi for each group that you wish to add to the car parking area.

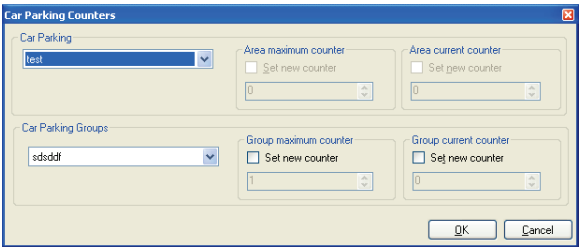
5.15.1 Viewing and Editing Car Parking Counters

Once you set up your various car parking groups and areas, these groups and areas can be easily viewed and edited.

To view and edit the Car Parking counters:

1. In the Events toolbar (above the Event Log area), click the icon.

   The *Car Parking Counters* window opens.



2. Update the maximum or current counters of either the car parking areas or the car parking groups, depending on how the car parking element is defined.

   The values of the maximum counters entered in this screen override the values of the maximum counters that you entered in Section 5.15.

3. Click **OK**.

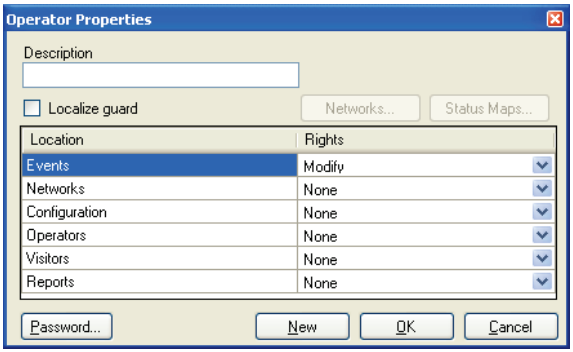
5.16 Adding Operators

Operators are people with access to the AxTraxNG™ application. The default operator name is Administrator.

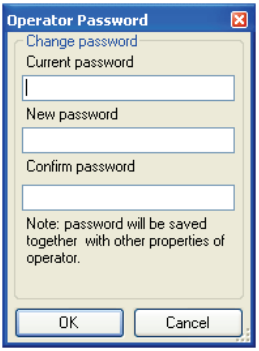
Different operators have wider or more restricted security rights, from complete control over the system to the ability only to view one section. All operator passwords are case-sensitive.

To define operators:

1. In the Tree View, expand the *Users* element and select **Operators**.
2. On the toolbar, click the icon.
   The Add *Operator* window opens.



3. In the *Description* field, enter the Operator's name.
4. Select the **Localize guard** checkbox to define the operator with limited rights.
5. Click **Networks…** and **Status maps…** to define the associated operator's local rights.
6. Set the operators global permission rights for each of the screens in the *Location* list.
7. Click **Password…** to open the *Password* dialog.



8. Enter the operators' password in the *Password* field and re-enter the password in the *Confirm Password* field.

> Note
> On first time use, leave the password field empty and enter (and confirm) your new password.

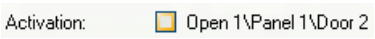
9. Click **OK** to save your settings.
   The dialog closes and the operator is shown in the display area.

5.17 Creating Elevator Control

Normally, a reader is associated with a door. For elevator control, a selected reader should be associated with outputs groups, with each output group representing a floor.

To create elevator control:

1. Select a reader (see Section 5.6) in the display area and click the icon.
2. In the *Reader Properties* window, clear the **Activation** checkbox.



3. Click **OK**.
4. Create output groups (see Section 5.10.3).
   Each output group represents a floor or several floors.

> Note
> When creating an output group for the elevator control, the selection only applies to outputs from the same panel.

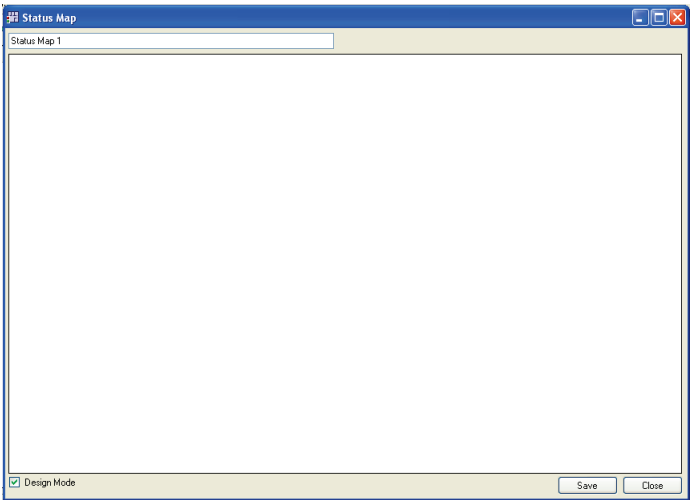
5. In the General tab of the User window, associate a user with the relevant output groups (see Section 5.12.2.1).
   Each user can be associated with the relevant output groups to allow user access to specific floors, as needed.
6. Create a panel link (see Section 5.9). Only one panel link is required.

5.18 Creating Status Maps

The Status Map displays the status of every door, input, and output, antipassback rules, and alarms in the facility on user-selected floor plans.

To set up a Status Map:

1. In the Tree View, select **Status Map** and click the icon.
   The *Add Status Map* window opens.



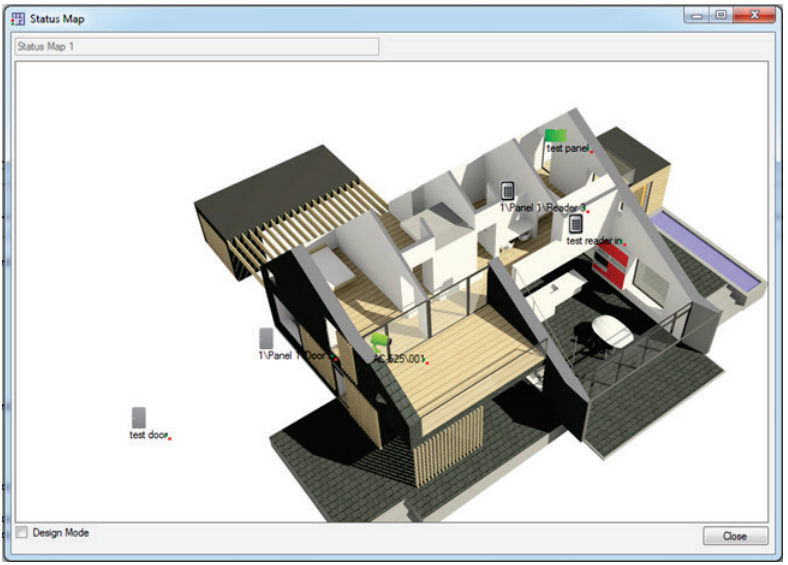
2. Right-click in the window and select **Set background** from the shortcut menu.

   The *Select Picture File* window opens.

Note

To change the map image and/or to add objects on the map, you must select the Design Mode checkbox. The **Add Map** icon in the toolbar is enabled.

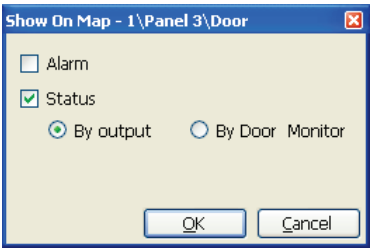
3. Select a graphic file (bmp, jpg, gif, or tiff) for the Status Map background.



4. Ensure that the Design Mode checkbox is checked.
5. Select readers, doors, inputs, outputs, additional status maps, cameras, or panels and click the **Add to Map** icon from the toolbar menu.

   The objects appear on the status map, and can be dragged to their correct position.
6. Right-click a map object and select **Show on Map** from the shortcut menu.

   The *Show on Map* window opens.



7. Select the **Status** checkbox to display the object's state on the status map.
8. For a door's Show on Map properties, select:
   a. **By Door Monitor**: Shows the doors open status based on its physical position.
   b. **By Output:** Shows the doors open status based on the status of its lock.
9. Select the *Alarm* checkbox to enable a visual alarm on the map for alarm events.

> **Note**
> The alarm option is only available for panel elements where the alarm was already defined.

10. Repeat Steps 5 to 9 until all objects are shown on the status map, as required.
11. Repeats Steps 1 to 9 to set up additional status maps.

> **Note**
> Status map icons can also be added to other status maps, indicating where the two map areas meet.

6. ViTrax™ Video Integration

ViTrax™ is a video management server client solution that supports AC-525, as well as a wide range of IP, USB, and open protocol cameras, such as OnVif and PSIA. For more information, see *ViTrax™ Software Installation Manual*.

Be sure that the ViTrax™ Server is installed on a PC and you know that PC's IP address. If not, refer to the *ViTrax™ Software Installation Manual* for installation instructions.

Perform the following steps to integrate the ViTrax™ server.

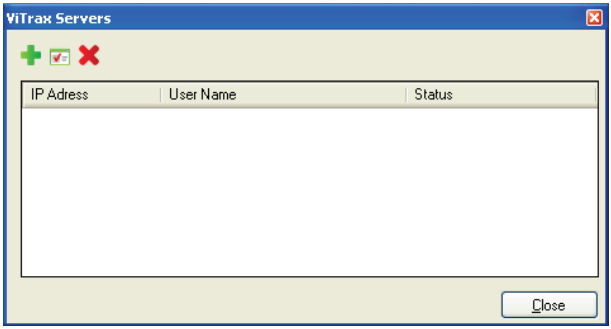
Step	Action	Section
1	**Connect to ViTrax™ Server**	6.1
2	**Add a Camera to AC-525 Panel**	6.2
3	**Linking a Camera to AxTrax**	6.3
4	**Use Panel Links**	5.9 and 6.4
5	**View Recorded Events**	6.5
6	**Use Automated Activation Options**	6.6

6.1 Connecting to ViTrax™ Server

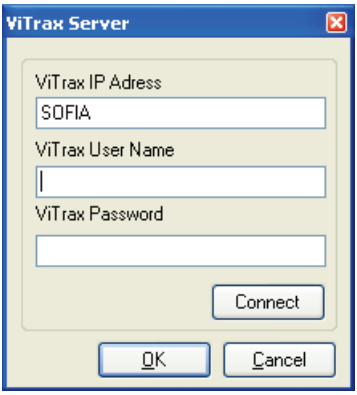
Define the ViTrax™ Server database with which the AxTraxNG™ Software communicates.

To connect to the ViTrax™ server:

1. When the ViTrax™ Server is running, click **File > ViTrax™ Server**.
   The *ViTrax™ Servers* window opens.



2. On the toolbar, click the icon.
   The *Add ViTrax Server* window opens.



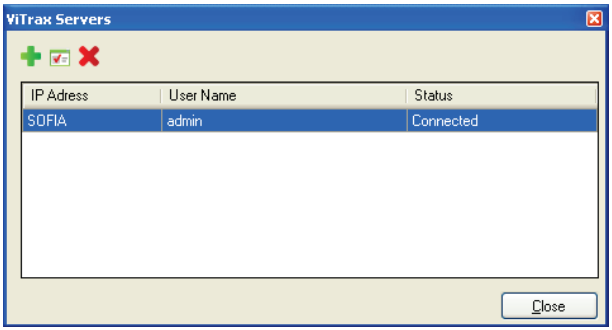
3. In *ViTrax IP Address*, enter either *"**localhost**"* or another IP address name.
4. In *ViTrax User Name*, enter the username.
5. In *ViTrax Password*, enter the password.

> **Note**
> The entered password must resemble the non-default password for the server.

6. Click **Connect**.
7. Click **OK**.

   When connected, the *Connected* status is displayed.

   The ViTrax™ server now appears in the *ViTrax Servers* window list.



6.2 Adding a Camera to the AC-525 Panel

Once a camera is physically installed, the system reads the camera on the network and displays it in the tree.

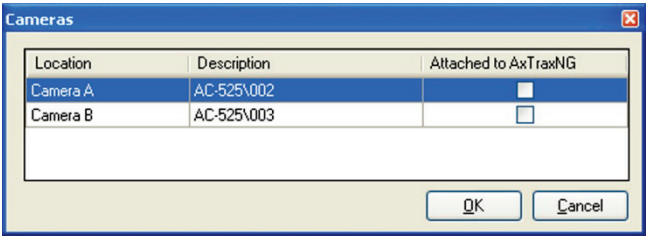
Defining communication of AC-525 cameras to the ViTrax™ server is performed physically between the camera and the AC-525 panel (see the *AC-525 Hardware Installation Manual*).

To view and add a camera to an AC-525 panel:

1. In the Tree View, click **AC Networks**.

   The available networks are listed in the display area.
2. Select a network.
3. Click the icon.

   The *Cameras* window opens.



4. Select the **Attached to AxTraxNG™** checkbox next to the camera you wish to add to the system.
5. Click **OK**.

For a detailed description of how to add a camera to the AC-525 panels as defined both in AxTraxNG™ and ViTrax™ applications, see Appendix E.

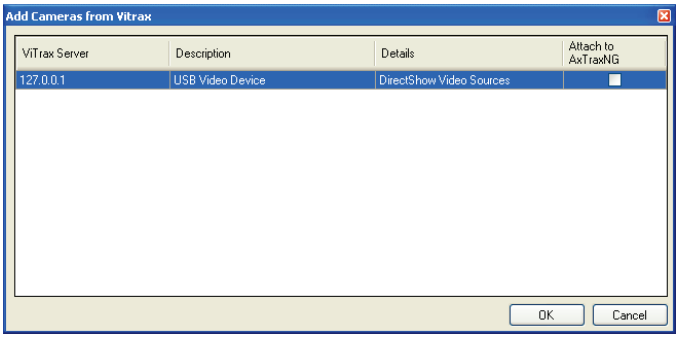
6.3 Linking a Camera to AxTrax

When a camera is linked to AxTrax, video events can be linked to access control events and vice versa.

To link a camera to AxTrax:

1. In the Tree View, select the *Camera* element.
2. On the toolbar, click the icon.

   A window opens showing all available IP (not AC-525) cameras that can be linked (cameras that have already been linked do not appear in this window).



3. For a camera you wish to link, select the **Attach to AxTraxNG** checkbox.
4. Click **OK**.

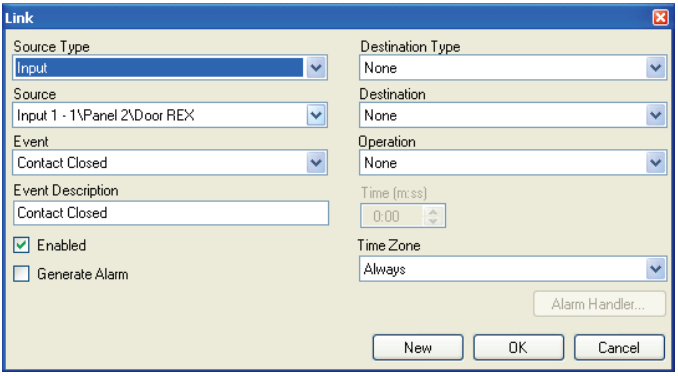
   The linked camera now appears in the Table View screen.

Note

You can also click the icon in the Events List to view the list of linked cameras.

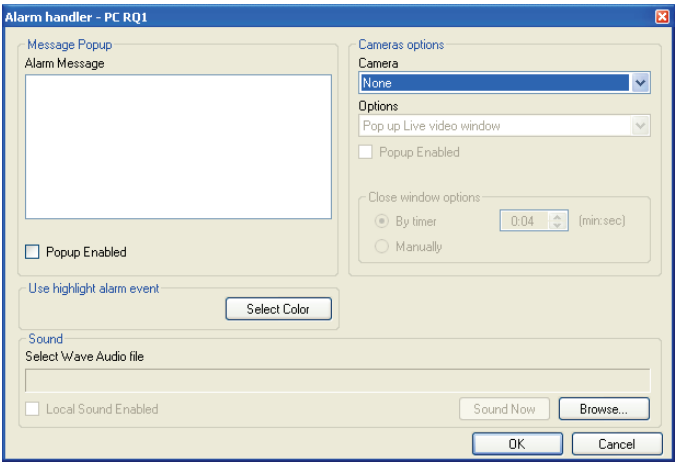
5. In the Tree View, click **AC Networks**.
6. Select a network and expand the panel to which you want to link the camera.
7. Select **AC Links.**
8. On the *Network* toolbar, click the icon.

   The *Add Link* window opens.

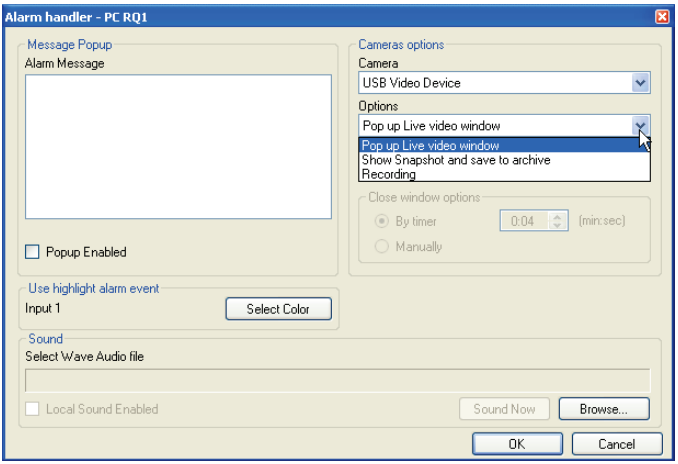


9. Select the **Generate Alarm** checkbox to activate the Alarm Handler button.
10. Click **Alarm Handler**.

    The *Alarm Handler* window opens.



11. From the **Camera** dropdown, choose the camera you wish to link.
12. From the **Options** dropdown, choose how the alarm is generated.



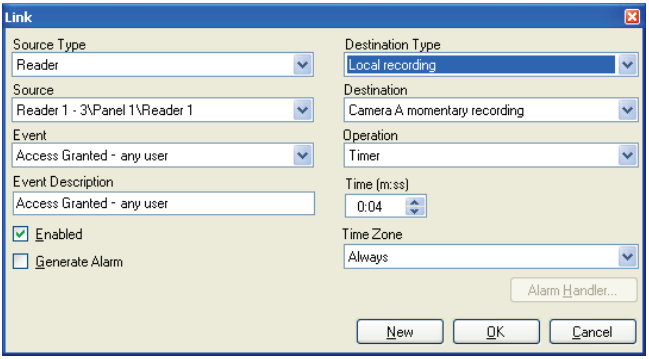
13. Click **OK** to close the *Alarm handler* window and return to the *Link* window.
14. Click **OK** to close the *Link* window and save the link rule configuration.

6.4 Conditioned Recording via Panel Links

You can select the source, destination, and period of recordings using Conditioned Recording sequences programmed via the *Panel Links* screen.

To create a panel link:

1. In the Tree View, click **AC Networks**.
   The available networks are listed in the display area.
2. Select a network and expand a panel in the Tree View.
3. Select **AC Links**.
4. Click the icon.
   The *Add Links* window opens.



5. In the **Destination Type** dropdown list, select **Local recording**.
6. In the **Destination** dropdown list, select a camera (momentary recording or pre-event recording).
7. Click **OK**.

6.5 Viewing Recorded Events

In the *Camera Properties* window, you can view live streaming and edit various camera properties.

The *Camera Properties* window includes the following:

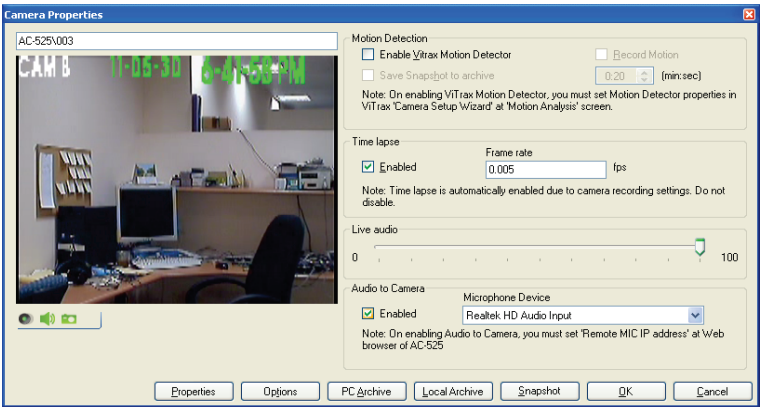
Table 18: Network > Panel > Cameras > Camera Properties Window

Field	Description
Description	Displays the camera name
Enable ViTrax Motion Detector	Select this checkbox to enable motion detection in ViTrax. Enabling motion detection enables Record Motion features. It is possible to get motion detection events from ViTrax™ and use them to initiate recording, by first setting the Motion Detection section on this window, and then setting motion detection properties in ViTrax™ in the *Sensitivity*, *Exclusion*, *Format*, and

Field	Description
	Source tabs.
Time Lapse	This checkbox is automatically enabled due to the camera recording settings. Time Lapse refers to the periodic recording of single frames. AxTraxNG™ automatically enables the Time Lapse option in ViTrax™ when setting recording by AxTraxNG™.
Frame rate	Select the Time Lapse period. By default, the Time Lapse period is 0.005 frames per second (1 frame every 200 seconds).
Live Audio Volume	Select the live audio volume
Audio to Camera	Select the checkbox to indicate when a microphone is connected to the camera.
Microphone Device	Enabled when the Audio to Camera checkbox is selected. From the dropdown list, select a microphone.
Properties	Camera properties
Options	Video pop-up window and snapshot options.
PC Archive	Streams saved in the PC
Local Archive	Streams saved in the USB-key
Snapshot	Opens the images list stored on the PC
Activation buttons	Start/Stop Recording, initiate Audio to camera, and Save current snapshot.

To access camera properties:

1. In the Tree View, click **AC Networks**.
   The available networks are listed in the display area.
2. Select a network and expand a panel in the Tree View.
3. Click the icon.
   The list of available camera appears in the display area.
4. Double-click the desired camera row within the camera list.
   The *Camera Properties* window opens.



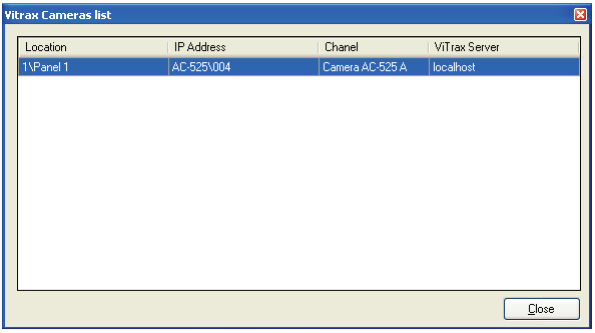
5. Click **OK**.

> Note
>
> The ViTrax™ Server must be running to view recordings.

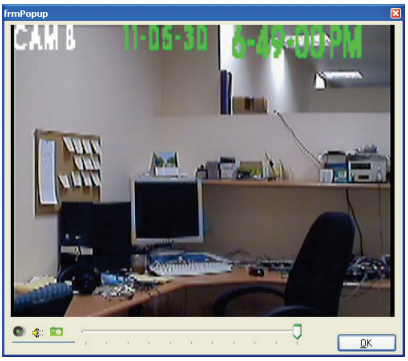
For more information on camera properties, see the *ViTrax™ Software Installation Manual*.

To access Live Video:

1. In the Events toolbar (above the Event Log area), click the icon.
   A list of all available cameras appears.



2. Double-click the desired camera row.
   The Live Video Streaming window opens.



The Live Video Streaming window includes the following buttons:

Table 19: Events Toolbar > Cameras > Live Video Streaming Window

Icon	Name	Click icon to...
	Recording	Starts/stops recordings that are saved as streams to the archive
	Audio to Camera	Use the PC microphone by utilizing the panel RAM
	Snapshot	Save the current snapshot.

3. Click **OK** to close.

6.6 Automated ViTrax™ Camera Activation Options

The following automated camera activation options are available in networks utilizing the ViTrax™ camera.

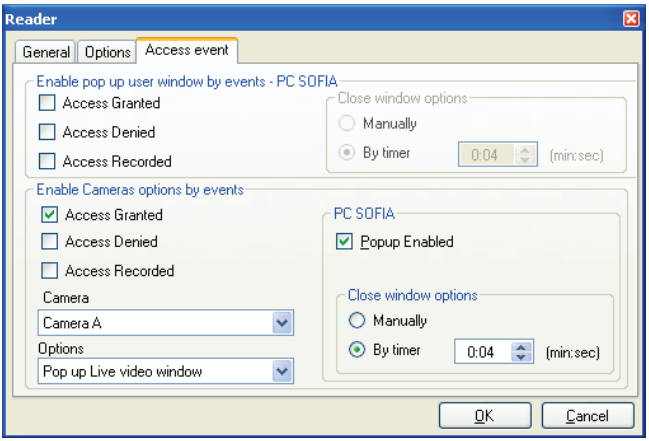
The automated camera activation turns on the camera and opens a video pop-up and a snapshot window on the locally used PC in response to predefined events occurring in the system as described in the following sections:

6.6.1 Reader Access

Create reader-access event based automatic camera activation on the local PC.

To create reader-access camera activation:

1. Open the *Reader* window (see Section 5.6).
2. Click the *Access event* tab.



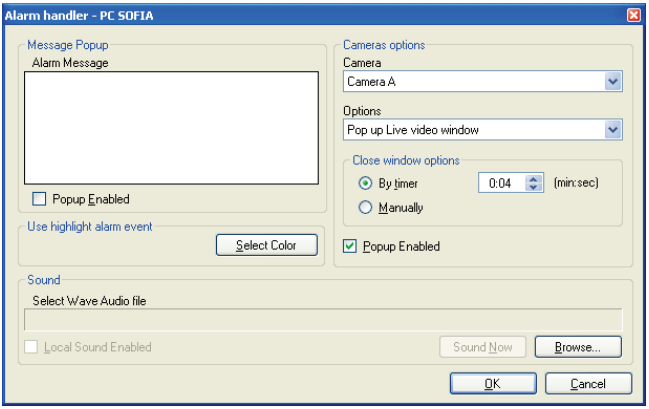
3. Under *Enable Camera options by events*, select the **Access Granted**, **Access Denied**, or **Access Recorded** checkbox.
4. Select a camera from the ***Camera*** dropdown.
5. Select a video option from the ***Options*** dropdown.
6. Select the **Popup Enabled** checkbox to enable local pop-up messages.
7. Under *Close window options,* select either **Manually** or **By timer**.
8. Click **OK**.

6.6.2 Alarm Event

Create alarm handler event based automatic camera activation.

To create alarm handler camera activation:

1. Open the *Alarm handler* window (see Section 5.9).



2. Select a camera from the ***Camera*** dropdown.
3. Select a video option from the ***Options*** dropdown.

4. Select the **Popup Enabled** checkbox to enable local pop-up messages.
5. Under *Close window options,* select either **Manually** or **By timer**.
6. Click **OK**.

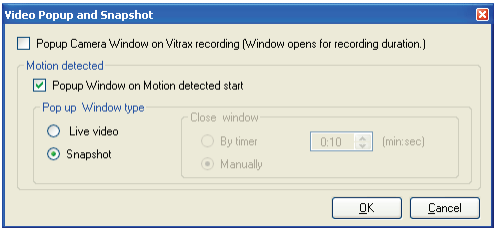
6.6.3 Camera Event

Create camera event based automatic camera activation.

To create camera event based camera activation:

1. Open the *Camera Properties* window (see Section 6.5).
2. Click **Options**.

   The *Video Popup and Snapshot* window opens.



3. Select the **Popup Camera Window on ViTrax recording** checkbox to enable window pop-up on the PC during camera's ViTrax™ recording.
4. Select the **Popup Window on Motion detected start** checkbox to enable window pop-up on the PC following an activation of the ViTrax™ Motion detection.
5. Under *Close window options,* select either **Manually** or **By timer**.
6. Click **OK**.

6.6.4 Door Warning Event

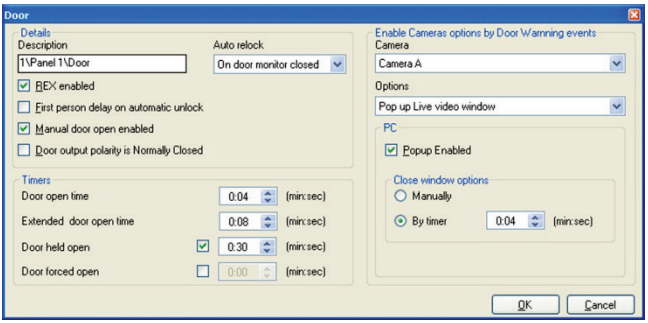
Create a door-warning event based automatic camera activation.

The available door warnings in the system are **Door held open** and **Door forced open**.

To create door-warning event based camera activation:

1. Open the *Door* window (see Section 5.5).
2. Select the **Door held open** and/or the **Door forced open** options, and define their associated timer.

   The *Enable Cameras Options by Door Warning Events* pane opens within the *Door* window.



3. Select a camera from the **Camera** List.
4. Select a video option from the **Options** list.
5. Enable local pop-up messages by checking the **Popup Enabled** checkbox.
6. Under *Close window options*, select either **Manually** or **By timer**.
7. Click **OK**.

7. Manual Operation

In addition to AxTraxNG™'s automated access control network monitoring and control, there is the option to manually control the network directly.

Door Manual Operation can only control doors that have been set as "Manual Door Open Enabled" in the *Door Properties* window (see Section 5.5).

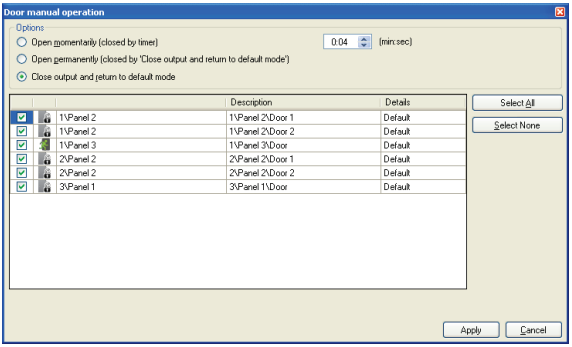
7.1 Controlling the Door Manually

The *Manual Door Operation* window allows an operator to open or close a selected group of doors directly.

To manually open or close a door:

1. In the Tree View, expand the **Networks** element and expand a selected network.
2. Expand a panel and select **Doors**.
3. On the toolbar, click the icon.

   The *Manual Door Operation* window opens.



4. Sort the listed panels/doors in regular or reverse order, by clicking the column header with the left mouse button.
5. Select an option:

   Open momentarily – Open all selected doors for the time set in the timer box

   Open permanently – **Opens a**ll selected doors

   Close output – Closes all selected doors and returns control to AxTraxNG™

6. Select the checkboxes of those doors to which to apply the operation.
7. Click **Apply**.

7.2 Changing the Reader Mode

The *Manual Reader Operation* window allows an operator to change the operation mode of a reader.

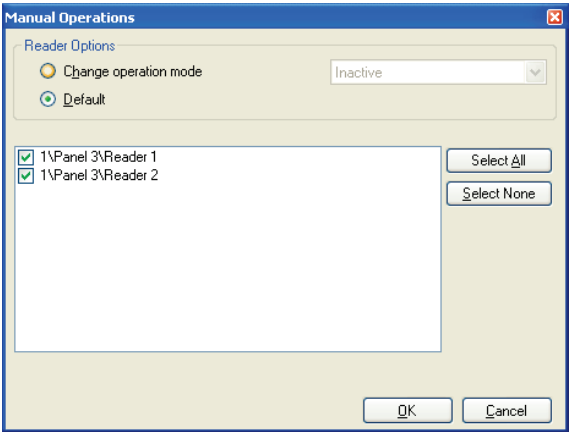
Readers have six possible operation modes:

- **Inactive:** The reader is not in use.
- **Card Only:** The reader accepts cards only.
- **PIN Only:** The reader accepts PIN inputs only.
- **Card or PIN:** The reader accepts both cards and PINs.
- **Desktop:** The reader is inactive, but can record new cards for the AxTraxNG™ database.
- **Secure (Card + PIN):** The reader requires first a card and then a PIN. The PIN must be entered within 10 seconds of the card.
- **No Access:** The reader does not grant access to users.

To change the reader mode manually:

1. In the Tree View, expand the **Networks** element and expand a selected network.
2. Select a panel.
3. Click the icon.

   The *Manual Reader Operation* window opens.



4. Select an option:
   - **Change operation mode** – Resets all selected readers to the selected operation mode.
   - **Default** – Returns control of the readers to the system.
5. Select the checkboxes of those readers to which to apply the operation.
6. Click **OK**.

For more information on secured (Card + PIN) time zones, see Section 5.6.1.

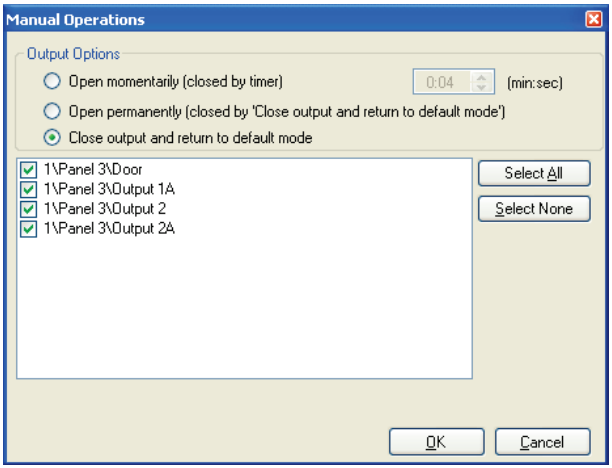
7.3 Controlling Outputs Manually

The Manual Output Operation window allows an operator to open or close a selected group of outputs on a panel directly.

To manually open or close an output:

1. In the Tree View, expand the **Networks** element and expand a selected network.
2. Select a panel.
3. Click the icon.

   The *Manual Output Operations* window appears.



4. Select an option:
   - **Open momentarily** – Opens all selected outputs for the time set in the timer box.
   - **Open permanently** – Opens all selected outputs.
   - **Close output and return to default mode** – Closes the selected outputs and returns control to default.
5. Select the checkboxes of the outputs to which to apply the operation.
6. Click **OK**.

7.4 Manually Disarming Inputs

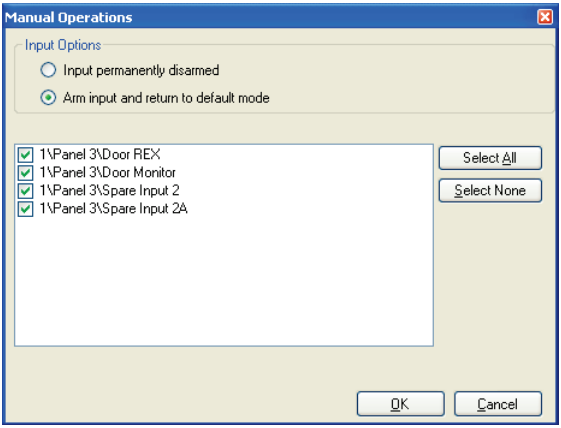
The *Manual Input Operation* window allows an operator to disarm a selected group of inputs directly on a panel.

An armed input means the input is active; a disarmed input is inactive and does not trigger any operation or alarms.

To manually disarm or rearm an input:

1. In the Tree View, expand the **Networks** element and expand a selected network.
2. Select a panel.
3. Click the icon.

   The *Manual Input Operations* window opens.



4. Select an option:
   - **Input permanently disarmed** – Deactivates all selected inputs.
   - **Arm input and return to default mode** – Reactivates the selected inputs and returns control to default.
5. Select the checkboxes of the inputs to which to apply the operation.
6. Click **OK**.

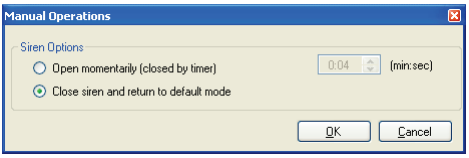
7.5 Controlling Sirens Manually

The *Manual Siren Operation* window allows an operator to test the siren for a selected panel.

To manually open or close a siren:

1. In the Tree View, expand the **Networks** element and expand a selected network.
2. Select a panel**.**
3. Click the icon.

   The *Manual Siren Operations* window opens.



4. Select an option:
   - **Open momentarily** – Sounds the siren for the time set in the timer box.
   - **Close siren and return to default mode** – Silences the siren and returns control to default.
5. Click **OK**.

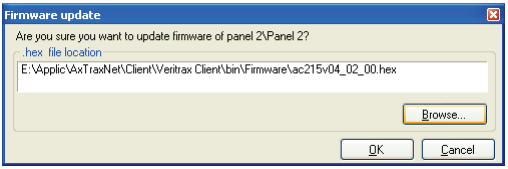
7.6 Manually Update Firmware

The *Update Firmware* window allows an operator to update the firmware version of the selected access control panel.

To perform a firmware update manually:

1. In the Tree View, expand the **Networks** element and expand a selected network.
2. Select a panel**.**
3. Click the icon.

   The *Update Firmware* window opens.



4. Click **Browse…** and select the HEX file relevant to the panel's hardware type.
5. Click **OK**.

8. AxTraxNG™ Reports

AxTraxNG™ supports two types of reports.

- Immediate Reports – List details of recent movements (within the last few hours). They are shown in the display area and can be exported.
- Archive Reports – List all events in the database.

8.1 Immediate Reports

There are four types of immediate reports:

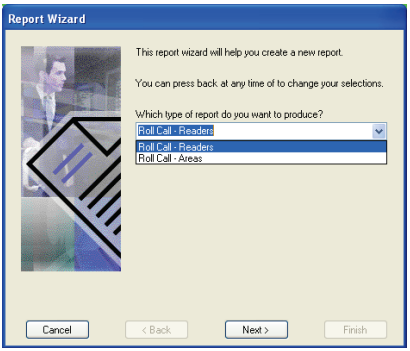
- **Who's been in today** – Lists where and at what time each user was granted access for the first time today.
- **Last known Position** – Lists where and at what time today each user was most recently granted access.
- **Roll-Call Readers** – Lists the last time each reader was given access, and by whom, within the last 1–99 hours.
- **Roll-Call Areas** – Lists all users currently within the selected area, sorted by department and entry time. The report lists all personnel who entered the facility within the last 1–99 hours.

To show an immediate report, select it from the Reports element of the tree-view, under Immediate.

To create a new immediate report:

1. In the Tree View, expand the **Reports** element and select **Immediate**.
2. On the toolbar, click the icon.

   The Report Wizard opens.


Report Wizard
This report wizard will help you create a new report.
You can press back at any time of to change your selections.
Which type of report do you want to produce?
Roll Call - Readers
Roll Call - Readers
Roll Call - Areas
Cancel
< Back
Next >
Finish

3. From the dropdown list, select a report type
4. Click **Next**.

   Follow the on-screen wizard instructions until the wizard has completed. The display area lists the new report.

8.2 Archive Reports

You can produce three types of reports:

- Panels Event Reports
- System AxTraxNG™ Events Reports
- Interactive Reports

8.2.1 Panels Events Reports

Panel event reports display details of all recorded panel events.

There are six available panel event reports:

- **Attendance Report –** Lists the attendance hours for selected users, sorted by date. Results include hours present, time in, and time out.
- **Panels Report** – Lists all the events recorded by the selected panels, sorted by date.
- **Access Report** – Lists all access events recorded by the selected readers, sorted by reader and date.
- **Readers Report** – Lists all users who have accessed the selected readers, sorted by department and date.
- **Fingerprint Report** – Lists specific fingerprints readers' events, sorted by reader and date.
- **Visitors Report** – Lists visitors who have made a visit to a certain user or department, or lists all related visitors.

8.2.2 System AxTraxNG™ Events Report

System AxTraxNG™ events reports list details of system and operator activity.

There are three available system event reports.

- **System Report** – Lists all operations performed by the AxTraxNG™ server, sorted by date.
- **Operators Report** – Lists all the operations performed by registered system operators, sorted by operation event type and date.
- **Alarm and Antipassback Handler Report** – Lists all raised system alarms, sorted by operator and date.

8.2.3 Interactive Report

Interactive reports list details of users and their access activity.

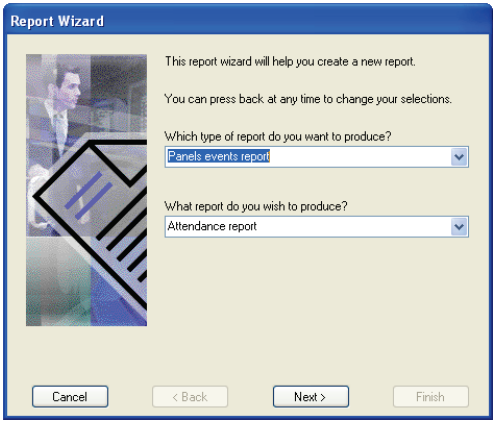
There are two available interactive reports:

- **User Access Rights Report** – Lists site access details for selected users, with full details of readers accessed and in which time zones.
- **Not Responding Users Report** – Lists users for whom there have been no access events for a selected period of time.

To create a new archive report:

1. In the Tree View, expand the **Reports** element and select **Archives**.

2. On the toolbar, click the icon.
   The Report Wizard opens.


Report Wizard
This report wizard will help you create a new report.
You can press back at any time to change your selections.
Which type of report do you want to produce?
Panels events report
What report do you wish to produce?
Attendance report
Cancel
< Back
Next >
Finish

3. From the first dropdown list, select a report type.
4. From the second dropdown list, select which report you wish to produce.
5. Click **Next**.
   Follow the on-screen wizard instructions until the wizard has completed. The display area lists the new report.

9. Administrator Operations

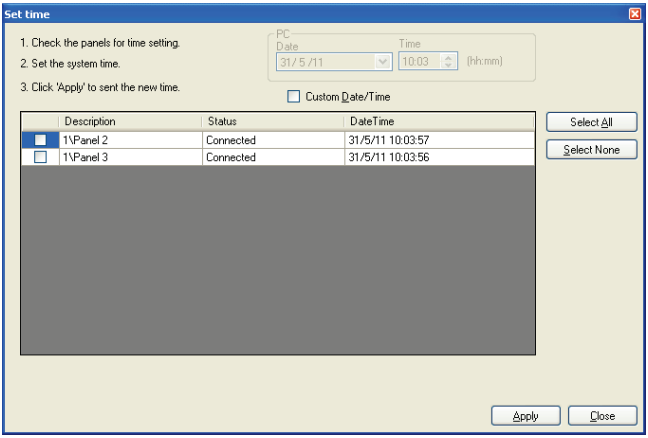
9.1 Setting the Time and Date

You can select panels by network and reset their date and time to the AxTraxNG™ server's system date and time, using the Set Time window.

To reset the panel time:

1. In the Tree View, expand the **Networks** element and select a network.
2. Click the icon.

   The *Set Time* window opens.



3. Select the panels to reset.
4. Click **Apply**.

   The server connects to the panels and sets the time as requested. A dialog confirms the operation.

9.2 Downloading Failed Data

In the event that some data fails to download to the access control panels, it is possible to perform a download of the failed operations only. You can perform this operation on a single panel, on all the panels in a network, or on all the panels in the entire system.

To download failed data:

1. In the Tree View, select a specific panel, a specific network, or all the networks.
2. Click the icon.

   The download data process begins.

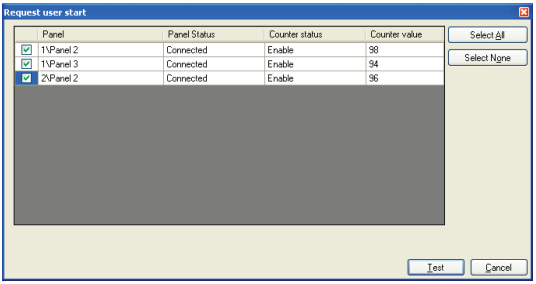
9.3 Testing User Counters

When using User Counters, it is possible to view the current User count value in each panel that has a Reader designated with the "Deduct User" option.

To view User Counters:

1. In the Tree View, select **Users > Department/Users or Users or Visitors**.
2. Select one user or visitor in the display area.
3. Click the icon.

   The *Request User Count* window opens.



4. Click **Test**.

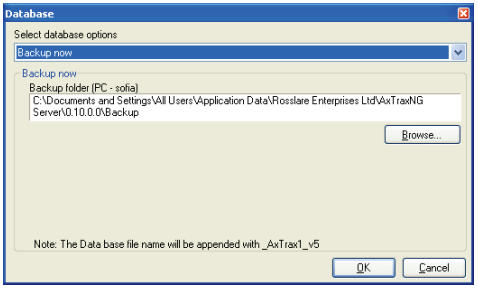
9.4 Maintaining the Database

Use the *Database* window to maintain the system database.

To open the Database window:

1. From the menu bar, select **Tools > Database**.

   The *Database* window opens.



The following database operations are available:

Table 20: Tools > Database > Available Databases

Operation	Description
Periodic Backup	Run a scheduled backup every specified number of days at the specified time.
Backup now	Run a one-time backup immediately.
Export Configurations and Events*	Copy the contents of the database to the selected folder.
Import Configurations*	Replace the current configuration based on the imported file.
Import Configurations and Events	Replace the current configuration and events based on the imported file.
Erase Configuration and Events*	Erase the current database configuration and all events.
Limit Panel Events Period	Automatically erase events when they are older than a specified number of days. Before using this option, Rosslare recommends that you set a periodic backup. **Note: It is recommended to set the value to no more than 91 days.**
Erase Panel Events	Erase all events that are older than a specified number of days.
Import database versions earlier than AS-225 VeriTrax or AS-525 AxTrax *	Replace the current database with VeriTrax AS-225 or AxTrax databases
Import database versions earlier than AxTraxNG	Replace the current database **Note: This option does not allow importing a database from a current AxTraxNG™ version.**

*This option is only available in the AxTraxNG™ Server PC.

The Backup and Export functions add the "_AxTrax1_vX" prefix at the end of exported or backed up database. The Import database function executes only with the string at the end of the file name. After a database is imported, the panel status may change to disabled. If this occurs, the operator should re-enable the panels.

9.5 AxTraxNG™ Options and Preferences

AxTraxNG™ can be customized to meet the preferences of the operator using the *Options* window.

To open the Options window:

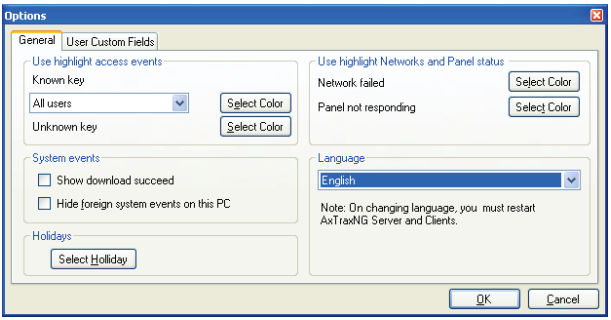
1. From the menu bar, select **Tools > Options**.

The Options window has two tabs:

- **General** – General startup and presentation settings
- **User Custom Fields** – Additional user-defined fields for the *User Properties* window

9.5.1 General Tab

The General tab includes presentation connection settings.



The *General* tab contains the following fields:

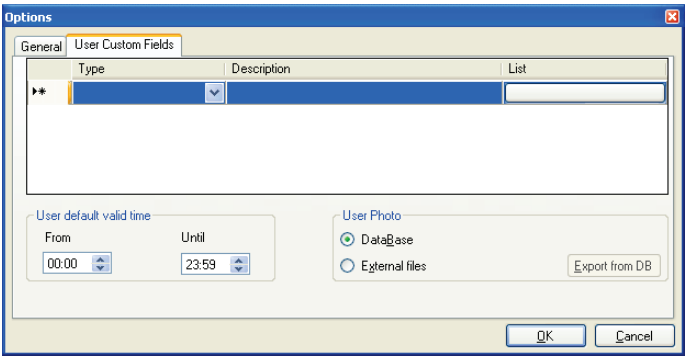
Table 21: Tools > Options > General Tab

Field	Description
Use highlight access events	From the **Known Key** dropdown, select the desired option and click **Select Color** to display selected user information in a custom picked colored highlight. Click **Select Color** adjacent to *Unknown key* to define the highlight color for unknown keys.
Show download succeed	Select the checkbox to add a message to the event history upon successful system parameters download from the AxTraxNG™ software to the panel.
Hide foreign system events on this PC	Select the checkbox to see only local administrator and AxTraxNG™ Server messages.
Select Holiday	Click the button to select Microsoft Outlook™ holidays to load into AxTraxNG™.

Field	Description
Use highlight networks and panel status	Click **Select Color** adjacent to *Network failed* to define the highlight color for network alarms. Click **Select Color** adjacent to *Panel not responding* to define the highlight color for panel communication errors.
Language	Select the system interface language. **Note: Setting the language to Farsi also changes the date format to the Farsi date format.**

9.5.2 User Custom Fields

The *User Custom Fields* tab controls the user-defined fields on the User Fields tab of the User Properties window. See Section 5.12.2.4.



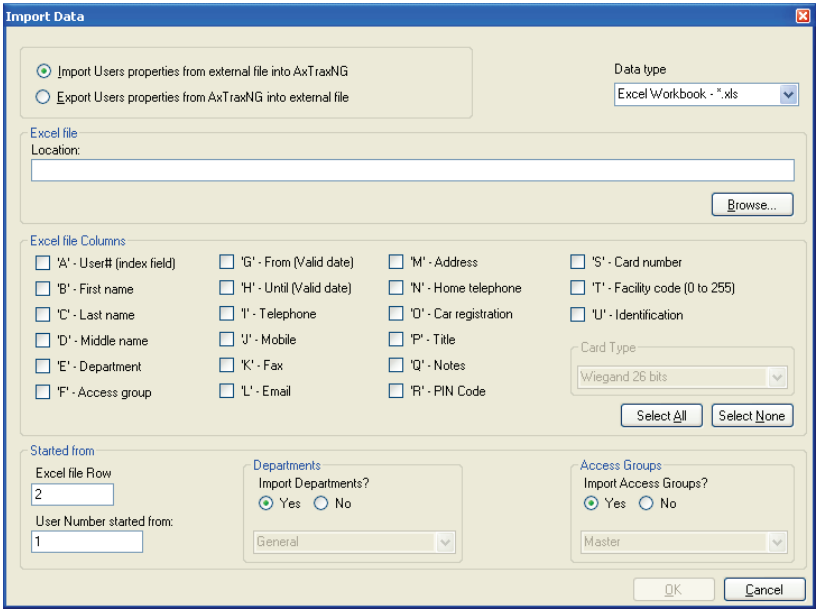
The *User Custom Fields* tab contains the following fields:

Table 22: Tools > Options > User Custom Fields Tab

Field	Description
Field type	Select the type of field. If field type is **list**, click **Edit** and enter list items.
Field description	Type a name for the new field.
User default valid time	Set default start and end time for user access rights using the **From** and **Until** fields.
User Photo	Define the default photos to be used: • **Database:** Use the User photos save in the Data base • **External files:** Use this option to save a large user photo collection external from the data base • **Export from DB:** Click to export existing photos from the Data base to an external folder

9.6 Importing/Exporting User Data

The Import/Export Data window makes it possible to import/export user information into/from the AxTraxNG™ database from/to a standard spreadsheet file.



The *Import/Export Data* window contains the following fields:

Table 23: Tools > Import/Export Data

Field	Description
Import Users Properties from external file into AxTraxNG™	Select this option to import user properties
Export Users Properties from AxTraxNG™ into external file	Select this option to export user properties
Data Type	Select the type of data file to import/export.
Location	Select the location of the file to import/export.
Browse	Click to select the file to import/export.
Excel File Columns	Select the checkboxes of the columns to be imported or exported. Data in each column (A–T) are imported or exported as listed.
Excel file Row	Enter the first row of user data in the spreadsheet.

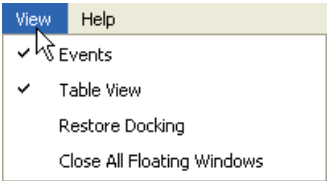
Field	Description
User number started from	Enter the number from which to start assigning unique system user numbers.
Import Departments?	Select **Yes** to import new departments into the AxTraxNG™ database. Select **No** to import users without their departments.
Department	Select the department to assign to the imported users. This box is only active when the *No* option is selected in the Import Departments option.
Import Access Groups?	Select **Yes** to import new access groups into the AxTraxNG™ database. Select **No** to import users without their access groups.
Access Groups	Select the access group to assign to the imported users. This box is only active when the *No* option is selected in the import access group option.

To open the Import/Export Data window:

1. From the menu bar, select **Tools > Import/Export Data**.

9.7 AxTrax GUI View Options

The AxTraxNG™ Client main window GUI can be customized using the *View* menu.



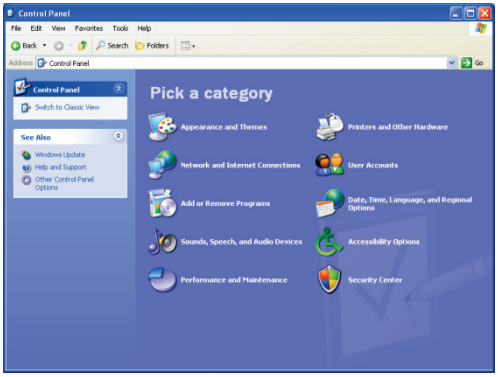
- **Events** to make Events window visible/invisible.
- **Table View** to make Table View visible/invisible
- **Restore** docking to return to default GUI Setting
- **Close all floating Windows** to close all pop-up windows.

A. Firewall Configuration

The following instructions explain how to configure the standard Windows Firewall for Windows XP.

To configure the firewall:

1. Open the Control Panel on your computer.



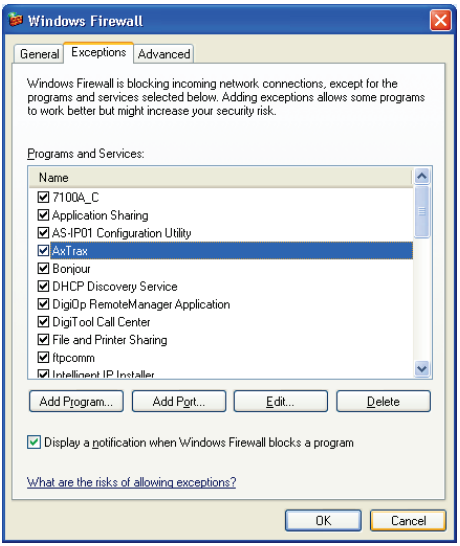
2. Click the **Security Center** category.

   The *Windows Security Center* window opens.

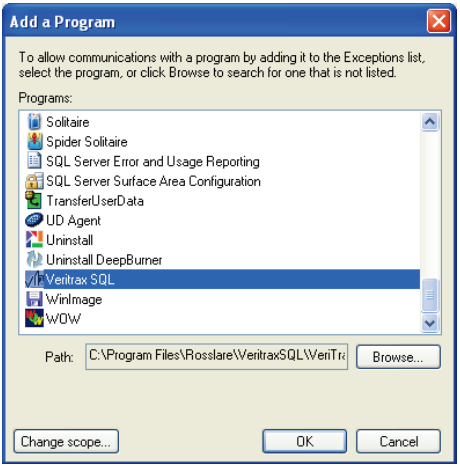
   (When in "Classic View", click the **Security Center** category in the top-left Control Panel preferences pane.)

Windows Security Center
Security Center
Help protect your PC
Resources
Get the latest security and virus information from Microsoft
Check for the latest updates from Windows Update
Get support for security-related issues
Get help about Security Center
Change the way Security Center alerts me
Security essentials
Security Center helps you manage your Windows security settings. To help protect your computer, make sure the three security essentials are marked ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel.
What's new in Windows to help protect my computer?
Firewall ON
Automatic Updates ON
Virus Protection ON
Manage security settings for:
Automatic Updates
Internet Options
Windows Firewall
At Microsoft, we care about your privacy. Please read our privacy statement.

3. Click **Windows Firewall**.
4. Select the *Exceptions* tab.



5. Click **Add Program**.
   The *Add a Program* dialog appears.



6. Click **Browse**.
   The *Browse* dialog appears.
7. In the **File Name** box, type:
   "**C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\BINN\sqlservr.exe**" and click **Open**.

8. Click **OK**.

   The SQL Server program appears in the Add a Program dialog.

9. Repeat Steps 6 and 7.

10. In the **File Name** box, type:

    "**C:\Program Files\Microsoft SQL Server\90\Shared\sqlbrowser.exe**" and click **Open**.

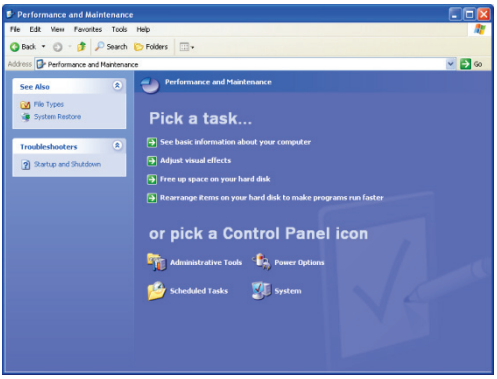
11. Click **OK**.

    The SQL Browser program appears in the Add a Program dialog.

12. In the Control Panel, click the **Performance and Maintenance** category.

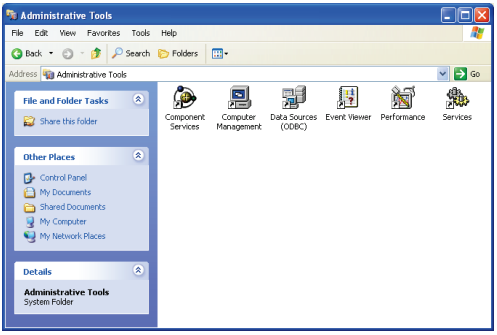
    (When in "Classic View", click **Switch to Category View** in the top-left Control Panel preferences pane, and then click the **Performance and Maintenance** category.)

    The *Performance and Maintenance* window opens.



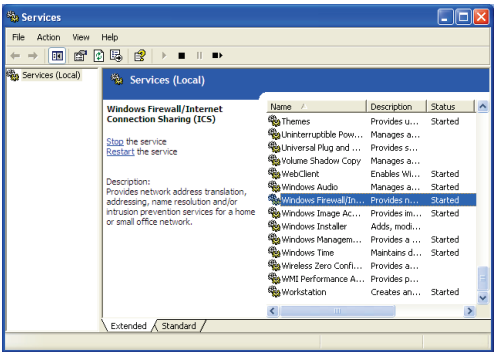
13. Click **Administrative Tools**.

    The Administrative Tools window opens.



14. Double-click *Services*.

    The Services Console opens.


Services
File Action View Help
Services (Local)
Services (Local)
Windows Firewall/Internet Connection Sharing (ICS)
Stop the service
Restart the service
Description:
Provides network address translation, addressing, name resolution and/or intrusion prevention services for a home or small office network.
Name
Description
Status
Themes Provides u... Started
Uninterruptible Pow... Manages a...
Universal Plug and ... Provides s...
Volume Shadow Copy Manages a...
WebClient Enables Wi... Started
Windows Audio Manages a... Started
Windows Firewall/In... Provides n... Started
Windows Image Ac... Provides im... Started
Windows Installer Adds, modi...
Windows Managem... Provides a ... Started
Windows Time Maintains d... Started
Wireless Zero Confi... Provides a...
WMI Performance A... Provides p...
Workstation Creates an... Started
Extended
Standard

15. Right-click **Windows Firewall/Internet Connection Sharing (ICS)** and click **Restart** from the pop-up menu.
16. Right-click **SQL Server** and click **Restart** from the pop-up menu.
17. Right-click **SQL Server Browser** and click **Restart** from the pop-up menu.

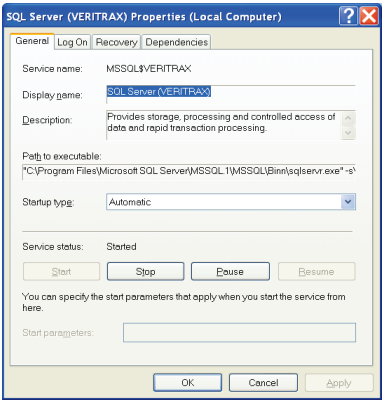
    The Firewall is now configured for AxTraxNG™.

B. SQL Service Settings

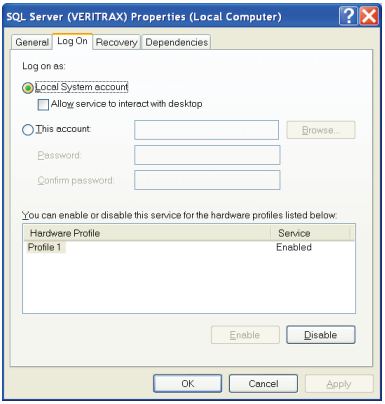
1. To reach the SQL Service Settings, click the following path from the Control Panel in Windows XP:

   Control Panel > Administrative Tools > Services and Applications > Services > SQL Server (VERITRAX)

2. Double click "**SQL Service (VERITRAX)**" the following dialog opens:



3. Under the General tab, verify that the Startup type is "Automatic" and that the Service status is "Started".



4. In the Log On tab, verify that the Local System Account radio button is selected. If not, select **Local System Account** and restart the computer for the changes to take effect.

C. Network Configuration

The AxTraxNG™ Server connects to access control units by a serial connection, a TCP/IP connection, or a Modem-to-Modem connection.

To connect access control panels to AxTraxNG™ over a TCP/IP LAN (Local Area Network) or WAN (Wide Area Network), the use of a TCP/IP to Serial converter is required, unless the panel has an onboard TCP-IP connection (AC-225IP or AC-525).

Each TCP-IP connection can support up to 32 access control panels that are connected to each other using RS-485.

The hardware used to connect to the TCP-IP network may be the MD-N32, which is a Serial to Ethernet converter, or using the onboard converter of AC-225IP or AC-525.

You can also use Rosslare's MD-N33 modem for a Modem-to-Modem connection. Refer to the hardware installation manuals of the desired panel for more details.

TCP/IP and Modem-to-Modem connections must be configured for use, and require expert knowledge of the local network.

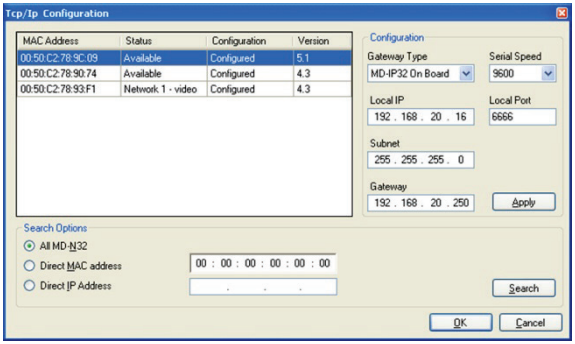
To configure TCP-IP Connection for AxTraxNG™:

1. In the Tree View, click **AC Networks**.
2. On the toolbar, click the icon. The Networks window opens.
3. Set the Network type as **TCP/IP**.

If you want to work with Remote, in the TCP/IP Network window select Remote (WAN), and add the WAN IP Address of the PC.

4. Click **Configuration**.

   The TCP/IP Configuration window opens.

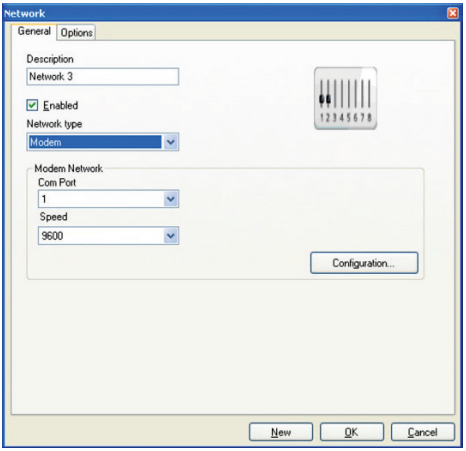


The upper left window lists all TCP/IP converters attached on the local network, identified by their MAC address, and indicates if they are available to be assigned to a new panel network or are already assigned.

5. From the MD-N32 list (the MD-N32's MAC address should be labeled on the TCP/IP converter), select the appropriate MAC address.
6. In **Gateway Type**, select the type of TCP/IP converter, MD-N32, MD-IP32 On board, or any other valid option. Skip this selection if it is already valid.
7. Type the **Local IP address** and **Subnet** for the computer's network.
8. Enter the **Local Port** number and select the **Speed** of your connection. It is recommended to select a higher value port number (4001 or higher). Note that the selected should not end with zeros (prefer setting Port value of 4243 rather than 4200). This avoids colliding with port addresses reserved for various equipment installed on the same network.
9. Click **OK** to start the verification process.
10. Turn off the MD-N32 power (or panel power if using the onboard module, such as MD-IP32), and then turn the power on again. This step is necessary when using certain versions of MD-N32 or MD-IP32 models. Skip this step if not applicable.
11. If configuration applies to a WAN network, disconnect the configured unit from the local network, and reconnect to the WAN network and access control panels network working over the WAN.

To configure MD-N33 in AxTraxNG™:

1. In the AxTraxNG™ software, add a new network.
2. Under network type, select **Modem**.



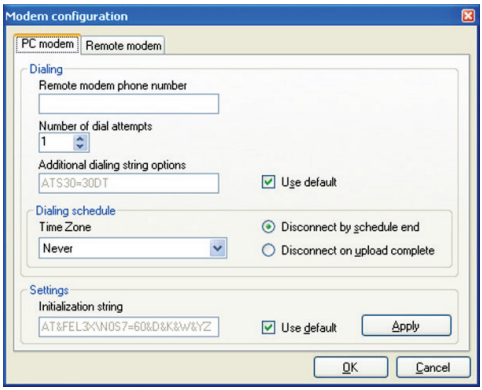
Note

Communication speed is limited to 9600, 19200, 57600, or 115200 bits per second.

To initialize and configure the computer modem:

1. In the Network window, click **Configuration**.

   The Modem Configuration window opens.



2. In the **Dialing** area, under **Remote modem phone number,** type the destination telephone number to call.
3. Click to change the **Number of dial attempts** (if required).

   For most applications, the default dialing string is sufficient.

   The dialing string is displayed in the window.
4. Clear the **Use default** checkbox. This allows adding or editing of the dialing string. Then, type the AT command in the **Dialing string** window.
5. From the **Dialing schedule** dropdown list, select the time zone.
6. Choose the disconnecting condition: **Disconnect by schedule end** or **Disconnect on upload complete**.

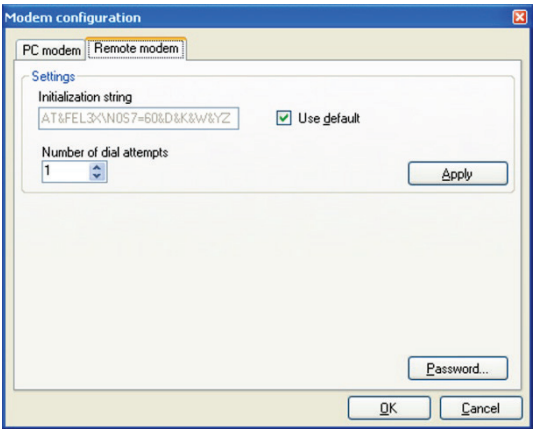
   This option is enabled when the selected time zone is different from the default time zone (Always and Never).
7. In the **Settings** area, the initialization string is displayed in the window. For most applications, the default initialization string is sufficient.
8. Clear the **Use default** checkbox to allow adding or editing of the dialing string. Then, type the AT command in the **Dialing string** window.
9. Connect the computer's modem to the PC via the selected COM port, and click **Apply** to initialize the PC modem.
10. Click **OK** to complete the initialization.
11. If the computer displays a failure message, check the modem connections and repeat the last steps.

Note

Remote modem initialization is at the PC side. When modem initialization fails through telephone line, a message appears.

To initialize and configure the remote modem:

1. In the Modem Configuration window, click the **Remote modem** tab.



2. In the **Settings** area, the initialization string is displayed in the window. For most applications, the default initialization string of is sufficient.
3. Clear the **Use default** checkbox to allow adding or editing of the dialing string. Then type the AT command in the **Dialing string** window.
4. In **Number of rings to answer**, set the number of rings before the computer modem answers.
5. Connect the remote modem to the computer via the selected com port, and click **Apply** to initialize the computer modem.
6. Click **OK** to initialize.
7. If a failure message appears, check the modem connections and repeat the last steps.

Note

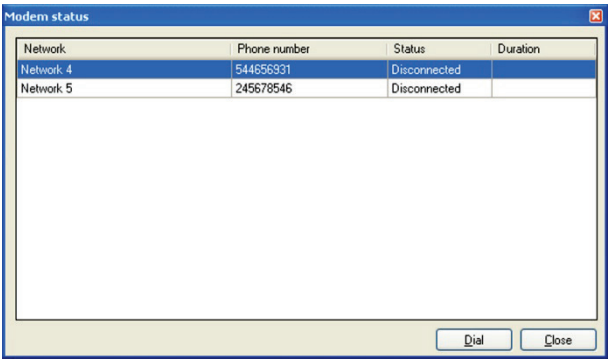
You must perform the action twice at the PC side, to Initialize two MD-N33s.

The MD-N33 and AxTraxNG™ software are now configured and ready.

You can now continue working using the AxTraxNG™ Adding New Panel procedure.

To check the remote modem status:

1. When a panel is setting in a modem network, you can see the status of the modem by clicking the **phone** icon in the toolbar.
2. There is a manual option to dial or disconnect the modem.



3. To prevent access to AxTraxNG™ data from non-authorized users, the AC-215, AC-225, AC-425 or AC-525 access control panels contain a password that can be changed only when the modem is connected and there is a link with the panel. You may be asked to enter the password during first data configuration, such as adding a new panel or downloading a new firmware.

D. Restoring Factory Default Settings

If the modem configuration password is lost or forgotten, reset the access control panel to the factory default settings, and use the default "VeriTrax" password.

Restoring factory default settings resets all doors and reader configurations to their factory defaults and clears all user properties.

To restore the factory default settings:

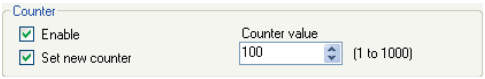
1. Turn off the supply power.
2. Disconnect all doors and readers wiring.
3. Connect Data 0, Data 1, and Tamper inputs to GND (-) in both reader 1 and 2 (total of six wires)
4. Power up the supply power for a few seconds. Wait for the "LED3" and "LED4" LEDs to flash alternately.
5. Turn off the supply power.
6. Connect the doors and readers wiring again.
7. In AxTraxNG™, delete the panel by clearing the **Enable panel** checkbox in the panel screen. Click **OK**.
8. Select the **Enable panel** checkbox in the panel screen and click **OK**. This action causes a full reset of the access control panel with the factory settings.
9. Dial to the appropriate access control panel and click **password** in the modem status screen. Use **AxTraxNG™** as the current password, and change the password to a new one.

E. Configuring User Counters

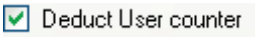
You can use the User Counter options to limit the number of entrances of a particular user. This is done using the Counter option that appears on the *User Properties* window (Figure 2 in Section 5.12.2).

To configure user counters:

1. Go the *General* tab of the *User Properties* window either as part of the procedure of adding a new user as described in Section 5.12.2, or select an existing user in the **Departments/Users** element and click the icon.
2. In the Counter section of the *User Properties* window, select the **Enable** checkbox.
3. Select the **Set new counter** checkbox and specify the number of allowed entrances for the user using the **Counter value** spin box.



4. Click **OK**.
5. Go the *General* tab of the *Reader Properties* (Section 5.6).
6. In the Details section, select the **Deduct User counter** checkbox.



7. Click **OK**.

E.1 Resetting Counter on Panel Re-enable

There is an additional counter option that allows you to reset the user counter to its starting value in the event that a panel is disconnected and then reconnected again.

If this option is not used, then upon panel re-enable, the user counter continues with its previous value prior to having that panel disabled.

To reset the user counter on panel re-enable:

1. In the Tree View, expand the **AC Networks** element and select a network.
2. From the Table View area, select a panel and click the icon.
   The *Panel Properties* window opens.
3. Click the *Options* tab.

4. Select the **Set new counter** checkbox.

5. Click **OK**.

F. Cross Platform Camera Setup

This section describes the complete process of adding cameras to the AC-525 panels as defined both in AxTraxNG™ and ViTrax™ applications, as well as emphasizes some of the important steps to help ensure proper camera operation.

This process is essentially a two-step procedure that needs to be defined in both applications.

First, you need to add the installed camera in the ViTrax™ software, only then is it possible to assign the camera to the relevant AC-525 panel defined in the AxTraxNG™ application.

To add a camera to the system:

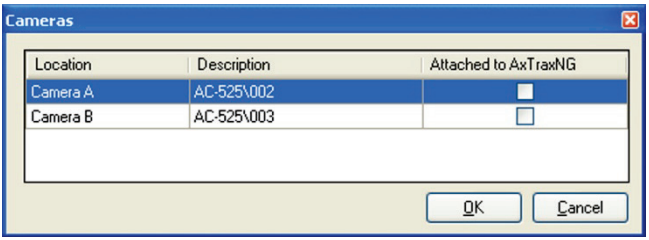
1. Install the AC-525 panel and connect the cameras (see AC-525 installation manual)
2. Add the camera in the ViTrax™ application by either:
   a. Performing a camera search using the **Automatically discover network devices** option.
   b. Manually add a camera using the **Camera setup wizard > Add new device** – **AC-525**.
3. [Optional] Configure Motion Detection in the ViTrax™ application if motion detection is used.

   If Motion Detection is required, first define Motion analysis via the ViTrax™ application:
   a. Select the **Use Motion Detector for the Stream Being Used** checkbox.
   b. Click **Properties** to adjust motion detection properties.

The Motion Detection feature consumes a large amount of CPU power, resulting in a high overall CPU power usage by the application. This may reduce the overall number of cameras that can be managed by the ViTrax™ Server application.

4. Add the camera in the AxTraxNG™ application:
   a. In AxTraxNG™, ensure that the ViTrax™ Server is configured and is "Connected" with AxTraxNG™.
   b. In the AxTraxNG™ Tree menu, select the relevant AC-525 Network item.
   c. Click the icon.

      On the left, you see the names of the cameras connected with this network as previously defined in ViTrax.



d. Select the **Attached to AxTraxNG™** checkbox next to the camera you wish to add to the system

e. Click **OK**.

5. Set the camera properties in the AxTraxNG™ application:

a. In the Tree View, click **AC Networks**.

b. Expand a network and select a panel to configure.

c. Click the panel's icon.

The available cameras are listed in the display area.

d. Select a camera row.

e. Click the Icon

The *Camera Properties* window appears.

6. Set the camera's time zone and daylight savings behavior from the *Camera* screen in the AxTraxNG™ application (Step 1):

a. In the *Camera Properties* screen, click the *Time* tab.

b. Select the local Time Zone from the dropdown list.

c. If Daylight Saving Time is now active, select the **Enable Daylight Saving Time** checkbox.

This advances the local time selected by 1 hour.

d. Click **Apply** or **OK**.

Note

Daylight savings is currently not updated automatically by Windows. It is therefore the user's responsibility to enable or disable the daylight saving time checkbox as necessary.

7. Set the camera's time zone and daylight savings behavior from the *Camera* screen in the AxTraxNG™ application (Step 2):

a. In the Tree menu double click a Panel item and Select the **Options** tab.

b. In the Time Zone section, define the time zone and Daylight Saving Time to match that of the *Camera* properties from Step 6).

8. Test time synchronization in both application:
   a. In the Tree menu, select your network and click the icon and verify that it matches the AxTraxNG™'s Server PC time.
   b. Select the panel and click **Apply** (1 or 2 seconds difference is acceptable).
   c. In the tree menu, double-click the icon and click **Properties**.
   d. Click the *Time* tab and verify that it matches the AxTraxNG™ Server PC time.
   e. If the ViTrax™ Server application and the AxTraxNG™ Server application are running on different PCs, ensure that both of the PCs are synchronized. It is advised that both PCs are assigned with the same time server.

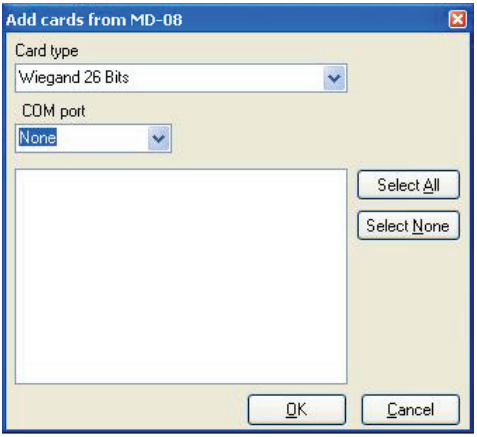
G. Enrolling Cards using MD-08 Desktop Reader

This option is available for users with the MD-08 unit on-board.

To define the MD-08:

1. Select **Cards** in the Tree View.
2. Click the **Insert card by MD-08** icon on the toolbar or click **Add from MD-08** on the *User form Codes* tab.

   The *Add Cards from MD-08* window opens.



3. Select the Card type and Com Port from the respective dropdown lists.
4. Enroll cards using the reader.
5. Click **Add.**

H. SQL Server Installation Troubleshoot

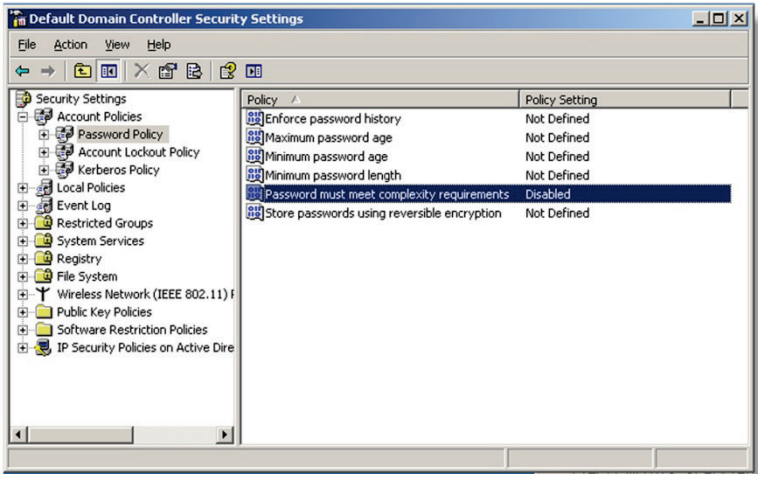
When installing the MS SQL Server 2005 Express component in a Windows Server (2003 or 2008) environment, you might get the following error message: "*The sa password must meet SQL Server password policy requirements.*"

This is because either:

- The domain-enforced policy is preventing the installer from setting the SA user's password, or
- The local security policy is preventing the installer from setting the password

You can temporarily disable this policy while the installation is running and click **Retry** to let the installation complete successfully. After installation is finished, you can restore the policy to the desired setting.

If you are on a Domain Controller, check the Domain Controller security settings first:

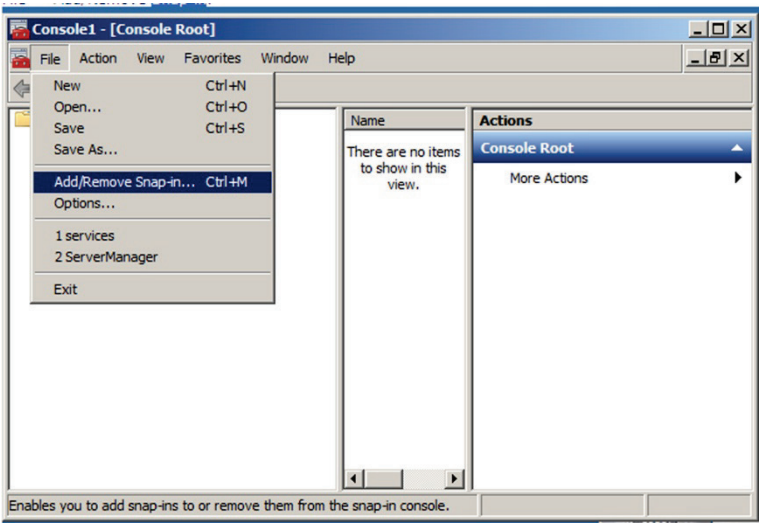


Note

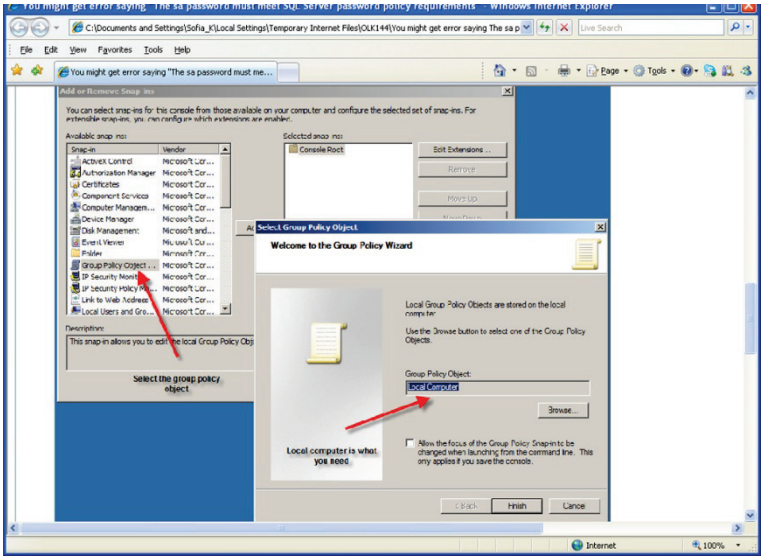
If the setting is set on a domain controller, you may need to run GPU date to force the changes to propagate.

If the server is not part of a domain, check the local security policy:

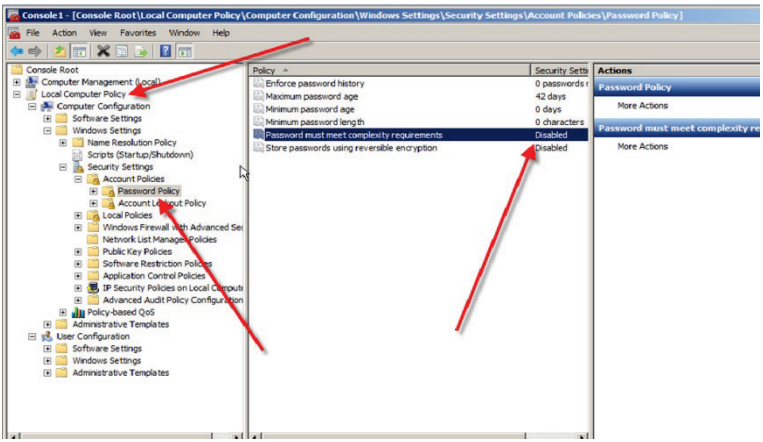
1. Open the MMC console: **Start -> Run -> mmc.exe**
2. Click **File -> Add/Remove Snap-in**:



3. Add the Group policy object for the Local Computer:



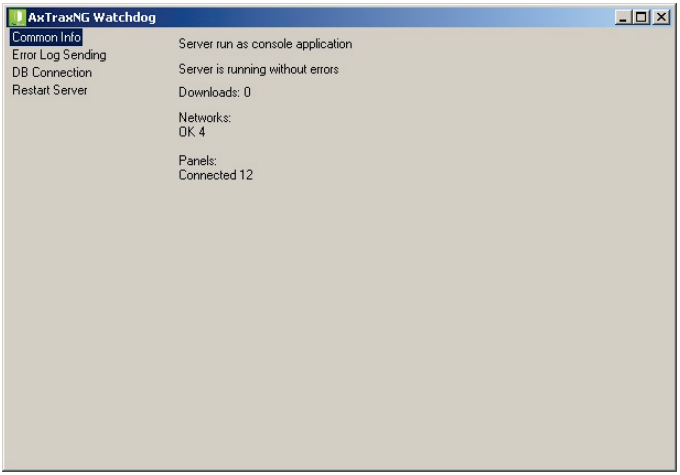
4. Disable (temporarily) the security policy:



I. AxTrax.NET Watchdog

The AxTrax.NET Watchdog is a program that monitors the AxTrax server.

Double-click the icon in the Window system tray to open the program.



The main window contains the following four topics:

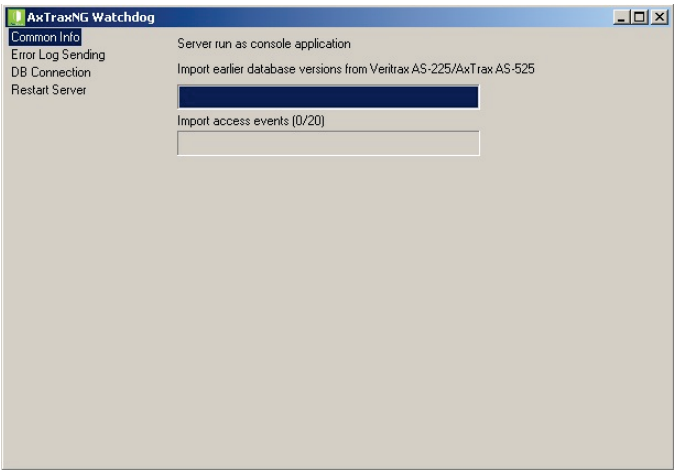
Common Info	Shows general system information
Error Log Sending	Sends error log to Rosslare Customer Support
DB Connection	Changes DB connection string **Note: Administrator password is required**
Restart Server	Restarts the AxTraxNG™ server **Note: Administrator password is required**

Once the main window opens, you can click on any of the three main topics to open that topic's screen.

I.1 Common Info

This screen shows general system information: server status, downloads counter, number of networks, number of panels, and networks and panels status.

In addition, if you import an earlier database from VeriTrax AS-225/AxTrax AS-525, the progress of the import is displayed in Common Info.



I.2 Error Log Sending

If you are experiencing problems with the server, you can use this function to send a report to Rosslare Customer Support for help.

The Error Log Sending screen contains following fields:

Table 24: Watchdog > Error Log Sending Screen

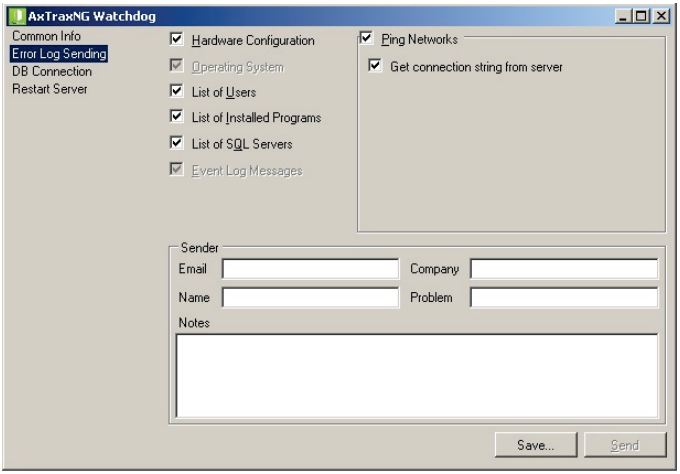
Hardware Configuration	Select this checkbox if you want to sends Hardware configuration with Error log
Operating System	Sends OS version with Error log
List of Users	Sends Users list with Error log
List of Installed Programs	Sends List of installed programs with Error log
List of SQL Servers	Sends List of SQL Servers with Error log
Event Log Messages	Sends Windows Event Log with Error log
Ping Networks	Sends network ping result with Error log
Get connection string from server	Sends connection string of DB with error log This option is enabled when Ping Network checkbox is selected.
SQL Server*	PC address with SQL server installed

Database*	DB name
Username*	Username of DB
Password*	Password of DB
AxTraxNG/Old AxTrax radio buttons*	DB of AxTraxNG™ of Old AxTrax
Sender section	
Email	Sender Email
Company	Sender Company
Name	Sender Name
Problem	Short description of problem
Buttons	
Save Button	Saves log to local machine
Send Button	Sends the log to Rosslare Customer Support

*These options are enabled when the **Get connection string from server** checkbox is cleared.

To send an Error Log report:

1. Click the **Error Log Sending** topic.
   The *Error Log Sending* screen is displayed.



2. Select the relevant checkboxes.
3. In the Sender section, fill out the necessary fields.
4. Click **Send**.

I.3 DB Connection

This feature allows you to change the database connection string.

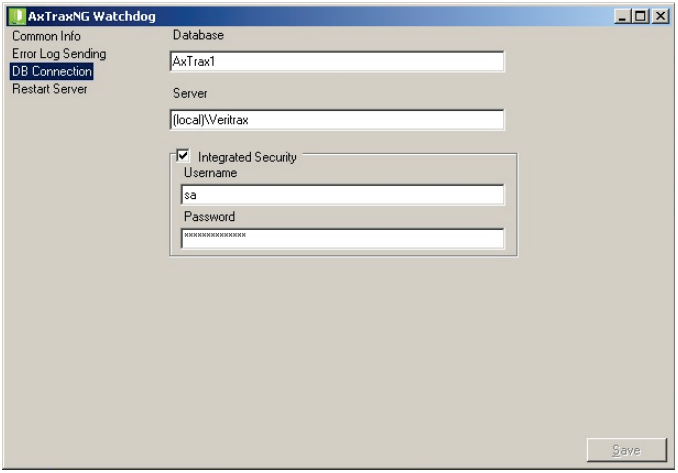
The DB connection window contains following fields:

Table 25: Watchdog > DB Connection Screen

Database	Database name
Server	DB Server path
Integrated security checkbox	Select this option to sends username and password of database
Username	Database username
Password	Database Password

To change the DB connection settings:

1. Click the **DB Connection** topic.
2. Enter the administrator password and click **OK**.
   The *DB Connection* screen is displayed.



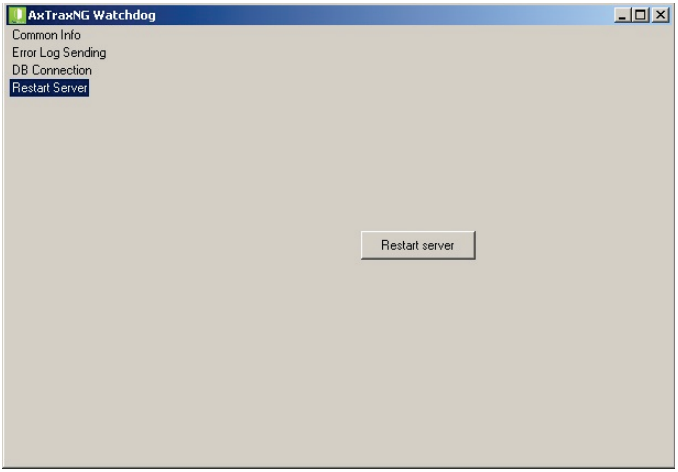
3. Change the field parameters as desired.
4. Click **Save**.

I.4 Restart Server

If you try to open the AxTraxNG™ Client but you get an error that the server is not connected, you may need to restart the server.

To restart the server:

1. Click the **Restart Server** topic.
   The *Restart server* button appears.



2. Click **Restart server**.
3. Enter the administrator password and click **OK**.
   The server restarts within a few seconds.

J. Adding Custom Wiegand Formats

The Wiegand protocol it the most common protocol between readers and controllers. This protocol is actually a collection of bits that represents the number of the user card ID.

There are many types of Wiegand protocols. Protocols differ from one another depending on the following three factors:

- The number of bits sent per card

  The most common format is 26-bit, but there are many more types such as 30-, 32-, 35- , and 36-bit.
- The representation of the user number

  In each card, there is a number that defines the user, but the representation of this number inside the Wiegand protocol can be changed. In addition, there is a Facility code in most protocols, which is not part of the number but is common to all users in this particular area. There are cards with additional codes such as Site code, but AxTraxNG™ recognizes them as a Facility code only. This means that if a card has both a Site code and a Facility code, AxTraxNG™ recognizes the first Facility code and the second Facility code is ignored.
- The authentication mechanism and its type inside the bit stream

  In most protocols, there is a certain type of authentication of the data transferred from the reader to the controller.

Once the user knows the format of the card, meaning how many bits there are per card, the user can use the other two factors to create new rules, which can then be enrolled into the software to teach the controller to understand the new format.

J.1 Representation

The following options are available when discussing the number representation:

- Card number is represented in a binary or hexadecimal code

  All the bits in the protocol are represented with 'D', which stands for data.
- Card number is represented in the protocol as a "reverse bytes". For example, if the number (hexadecimal) is 34 65 89 32, then it is represented as: 32 89 65 34.

  All the bits in the protocol are represented with 'R'.
- Card number is represented in the protocol as a "reverse bits". For example, if the number (hexadecimal) is 34 65 89 32, which is represented in binary code as:

  00110100 01100101 10001001 00110010

then in reversed bits format, it is 4C 91 A6 2C, which is represented as: 01001100 10010001 10100110 00101100 in binary.

All the bits in the protocol are represented with 'Z'.

- Card number is represented in the protocol as a BCD code (each nibble represents one decimal character). For example, if the number (decimal) is 658723, then it is represented in binary as: 01100101 10000111 00100011.

  All the bits in the protocol are represented with 'B'.

J.2 Facility Code

If supported in the card, the software must know where it is placed inside the bit array and how many bits it takes.

Of the 5 representation options presented in J.1, only the data format can be used with the Facility code; however, all the bits in the protocol are represented with 'F' to differentiate it from regular data.

J.3 Authentication

Usually the array of bits that represents the card number also contains an authentication mechanism that checks that the data was transferred correctly.

AxTraxNG™ supports several types of authentication mechanisms as follows:

- Even Parity – One bit provides authentication to either several bits proceeding or following it (according to the defined protocol). This bit makes the total number of related bits an even number.

  The Even Parity bits in the protocol are represented with 'E' and all the bits that they verify are represented with '1'.

- Odd Parity – One bit provides authentication to either several bits proceeding or following it (according to the defined protocol). This bit makes the total number of related bits an odd number.

  The Even Parity bits in the protocol are represented with 'O' and all the bits that they verify are represented with '1'.

- CheckSum – The number of bits (usually 8) provides the sum of the previous bytes.

  Checksum bits in the protocol are represented with 'S' and all the bits that they verify are represented with '1'.

- CheckXor – The number of bits (usually 8) provides a logical XOR value of the sum of the previous bytes.

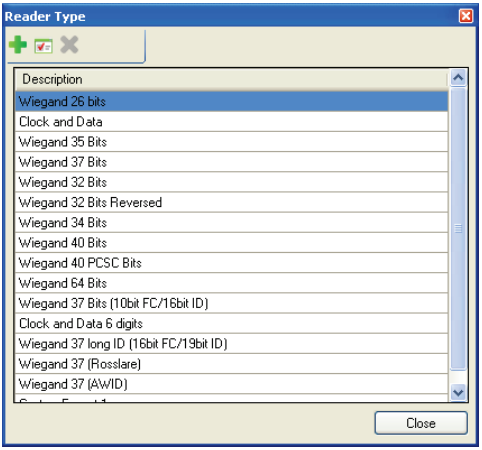
  CheckXor bits in the protocol are represented with 'X' and all the bits that they verify are represented with '1'.

J.4 Creating New Rules

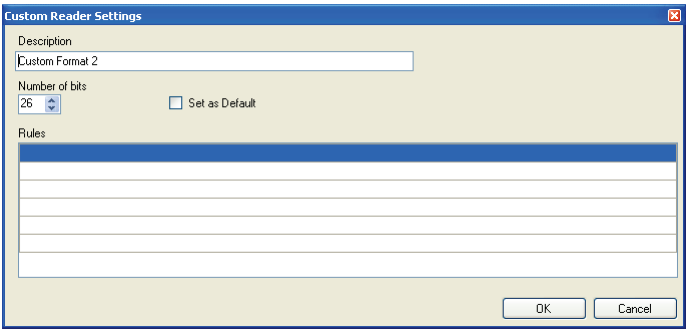
Using the above principles, we can create new rules for the AxTraxNG.

To create a new rule:

1. In the Tree View, click **AC Networks**.
2. Click **Reader Type** icon.
   The Reader Type window opens.



3. Click the icon.
   The *Custom Reader Settings* window opens.



4. In Description, Enter a description of the new rule.
5. Choose the number of bits the new rule will use.
6. Select the Set as Default checkbox.
7. In the Rules section, enter the protocol rules according to the guidelines described in Sections J.1 through J.3 and as shown in the example below.

Note

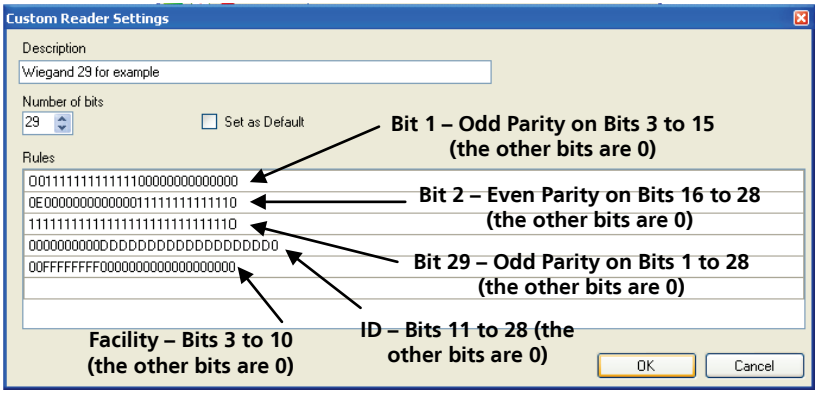
The protocol definition is for the entire system and not per controller.

Example

Enter a new Wiegand 29-bit protocol with the following rules:

- Rule 1: Bit 1 – Odd parity on the bits 3–15
- Rule 2: Bit 2 – Even parity on the bits 16– 28
- Rule 3: Bit 29 – Odd parity on the bits 1–28
- Rule 4: Bits 11–28 – ID data
- Rule 5: Bit 3–10 – Facility code

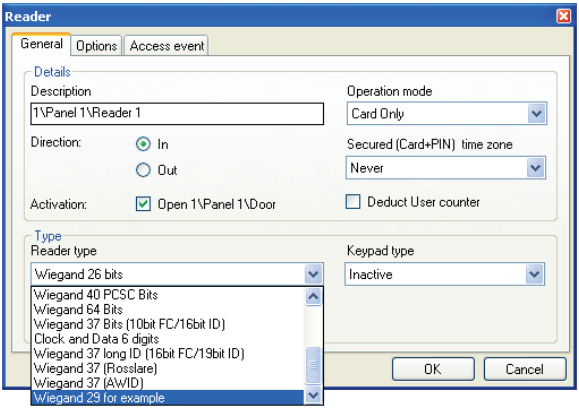
The new protocol appears in the *Custom Reader Settings* window.


Custom Reader Settings
Description
Wiegand 29 for example
Number of bits
29
Set as Default
Rules
Bit 1 – Odd Parity on Bits 3 to 15 (the other bits are 0)
Bit 2 – Even Parity on Bits 16 to 28 (the other bits are 0)
Bit 29 – Odd Parity on Bits 1 to 28 (the other bits are 0)
ID – Bits 11 to 28 (the other bits are 0)
Facility – Bits 3 to 10 (the other bits are 0)
OK
Cancel

Note

Please note that the first character in the first row and the last character in the third row, which represents the odd parity, is a capital "O" and not a zero (0).

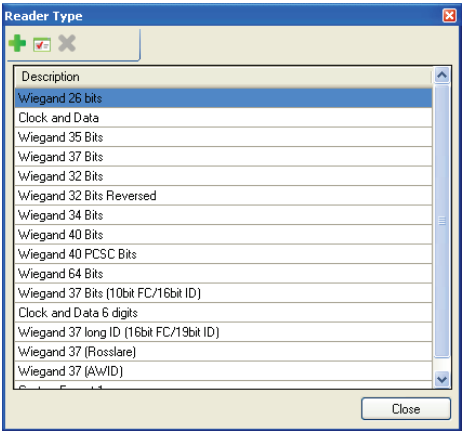
The new protocol now appears in the list of available protocols.



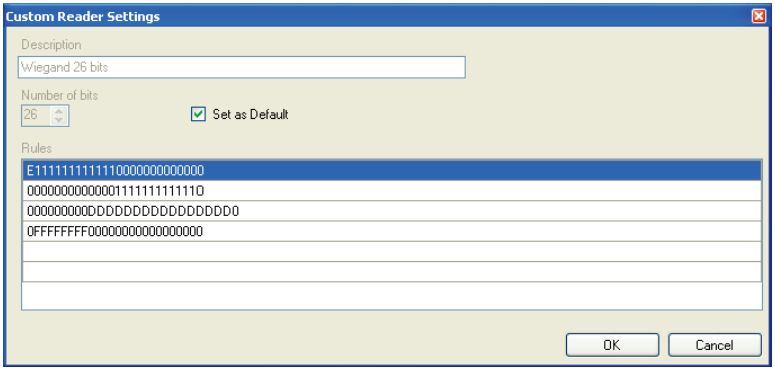
The representation of each existing protocol can be viewed.

To view the format of existing protocols:

1. In the Tree View, click **AC Networks**.
2. Click **Reader Type** icon.
   The *Reader Type* window opens.



3. Double click protocol you wish you view (in this case, Wiegand 26-Bit). Alternatively, you can choose the protocol you wish to view and click the icon.
   The *Custom Reader Settings* window opens.



Note

The protocol representation is for viewing only and cannot be edited.

For help in creating a new protocol, please refer to Customer Support.

AxTraxNG™

Asia Pacific, Middle East, Africa

Rosslare Enterprises Ltd.
Kowloon Bay, Hong Kong
Tel: +852 2795-5630
Fax: +852 2795-1508
support.apac@rosslaresecurity.com

United States and Canada

Rosslare Security Products, Inc.
Southlake, TX, USA
Toll Free: +1-866-632-1101
Local: +1-817-305-0006
Fax: +1-817-305-0069
support.na@rosslaresecurity.com

Europe

Rosslare Israel Ltd.
Rosh HaAyin, Israel
Tel: +972 3 938-6838
Fax: +972 3 938-6830
support.eu@rosslaresecurity.com

Latin America

Rosslare Latin America
Buenos Aires, Argentina
support.la@rosslaresecurity.com

China

Rosslare Electronics (Shenzhen) Ltd.
Shenzhen, China
Tel: +86 755 8610 6842
Fax: +86 755 8610 6101
support.cn@rosslaresecurity.com

India

Rosslare Electronics India Pvt Ltd.
Tel/Fax: +91 20 40147830
Mobile: +91 9975768824
sales.in@rosslaresecurity.com

ROSSLARE
SECURITY PRODUCTS
www.rosslaresecurity.com

0706-0960417+00

TÜVRheinland CERT ISO 9001 ISO 14001

EN ISO 13485

RoHS COMPLIANT

CE